Universidade do Minho

Licenciatura em Ciências da Computação

Sistemas de Comunicações e Redes

TP1: Nível de Ligação Lógica - Ethernet e Protocolo ARP; Redes Sem Fios (IEEE 802.11)

(3 aulas)

1. Objetivos

Este trabalho, previsto para três aulas, tem duas partes distintas. Na primeira parte pretende-se explorar explorar a camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP (*Address Resolution Protocol*). O protocolo ARP (ver RFC 826 em https://www.rfc-editor.org/rfc/rfc826.html) 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.

Na segunda parte, procura-se 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.

Parte 1: Nível de Ligação Lógica - Ethernet e Protocolo ARP

2. Introdução

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 de ligação física.

O serviço mais básico prestado pela camada de ligação lógica é a transferência de dados de um nó para os nós imediatamente adjacentes na topologia da rede. No nó de origem cada unidade protocolar da dados (*Protocol Data Unit* (PDU)) do nível de rede (*e.g.*, datagrama IP) é encapsulada numa trama de nível de ligação, sendo depois enviado através da camada física para o nó destino. No destino, o nó recebe a trama do nível físico, extrai o pacote IP (datagrama) 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). Estes serviços podem ser oferecidos por outros níveis da pilha protocolar, por exemplo, o nível de transporte com o protocolo TCP *(Transmission Control Protocol)*, que é um protocolo de transporte fiável usado na Internet. 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 nos 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 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 (B_1). Nessa altura, o recetor compara B com B_1. 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 B_1 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 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.

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 receptor 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 entre os nós pode haver colisões entre tramas transmitidas simultaneamente por dois ou mais nós. Quando há uma colisão de tramas é muito improvável que os recetores receberem 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 testemunho (*token-based*) e protocolos de acesso aleatório. Em particular, estes últimos são os mais usados nas redes locais. 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 de *hardware* ou 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; senão, 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.

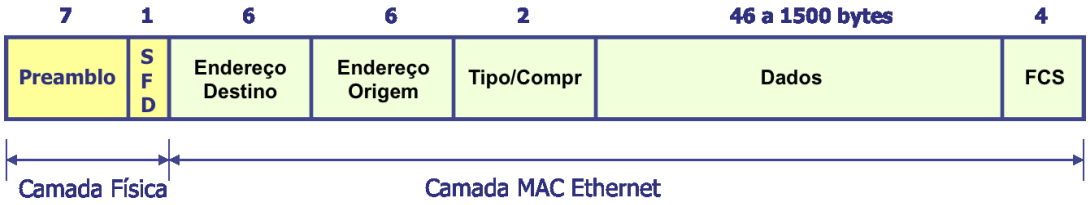
Note que o protocolo ARP tem um âmbito de operação restrito à rede local. Quando o destino IP é remoto, o protocolo ARP é usado para determinar o endereço MAC da interface do *router* que está na mesma rede local, router esse que, por sua vez, tem possibilidade de determinar qual o caminho que o datagrama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

Ethernet

Ethernet é uma tecnologia de rede local bastante popular, havendo 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 que será detalhado nas aulas teóricas, e usa um formato de trama simples que inclui campos de controlo e um campo de dados.

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 (*payload*); e (vi) o campo FCS (*Frame Check Sequence*) para 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*).

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 chega uma trama Ethernet a uma interface é comutada de imediato para a interface apropriada. O preenchimento da tabela é feito através de um mecanismo de auto-aprendizagem. 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. Quando chega uma trama que o *switch* não consegue comutar com base na tabela de comutação difunde-a através de todas as suas interfaces.

Por sua vez os *routers*, estudados no trabalho anterior, funcionam ao nível de rede encaminhando pacotes IP (ou datagramas IP) com base no endereço IP destino, 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.

3. Captura e Análise de Tramas Ethernet

A captura de tráfego deverá ser efetuada usando a aplicação Wireshark instalada na **máquina nativa**. Uma vez que as salas de aula atuais não disponibilizam uma ligação com fios a uma rede Ethernet, a captura será realizada na rede Eduroam. Este facto não impacta na realização do trabalho porque, por defeito, o Wireshark disponilibiliza o tráfego capturado ao utilizador como sendo (pseudo) Ethernet.

Assegure-se que a *cache* do seu browser está vazia, ou então aceda à página *web* pretendida usando o *hard refresh*, o qual permite limpar a cache do *browser* para uma determinada página, forçando o *browser* a carregar a última versão da página existente no servidor. Normalmente o *hard refresh* duma página faz-se com CTRL+F5, mas caso não funcione, procure na Internet a forma de fazer *hard refresh* no seu *browser*.

Ative o Wireshark na sua máquina nativa.

No seu *browser*, aceda ao URL *http://www.scom.uminho.pt*.

Pare a captura do Wireshark.

Obtenha o número de ordem da sequência de bytes capturada (coluna esquerda (No.) do Wireshark) correspondente à mensagem `HTTP GET` enviada pelo seu computador para o servidor Web, bem como o começo da respectiva mensagem `HTTP Response` proveniente do servidor (use o filtro http).

No sentido de proceder à análise do tráfego, selecione a trama Ethernet que contém a mensagem HTTP GET. Recorde-se que a mensagem GET do HTTP está no interior de um segmento TCP que é transportado num datagrama IP que, por sua vez, está encapsulado no campo de dados duma trama Ethernet. Expanda a informação do nível da ligação de dados e observe o conteúdo da trama Ethernet (cabeçalho e dados (*payload*)).

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem HTTP GET.

Sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada. Para imprimir um pacote, use File→Print, escolha *Selected packet only* e *Packet summary line*, ou use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o detalhe necessário para responder às perguntas.

1. Anote os endereços MAC de origem e de destino da trama capturada.

2. Identifique a que sistemas se referem. Justifique.

3. Qual o valor hexadecimal do campo `Type` da trama Ethernet? O que significa?

4. Quantos bytes são usados desde o início da trama até ao caractere ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (*overhead*) introduzida pela pilha protocolar no envio do HTTP GET (considere o FCS).

A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP.

5. Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.

6. Qual é o endereço MAC do destino? A que sistema corresponde?

7. Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.

4. Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP. Para tal, inicie o **emulador CORE** com o comando "sudo core" e mantenha-o ativo até ao final da Parte 1.

Em modo de edição crie a seguinte intranet com dois departamentos, *A* e *B*. O departamento *A* usará os endereços 192.<nº do grupo>.<nº do grupo>.X/24, e o departamento *B* 192.<nº do grupo+1>.<nº do grupo+1>.X/24, sendo X o decimal

atribuído automaticamente pelo CORE. Por exemplo, o grupo G11 usará os endereços 192.11.11.X/24 e 192.12.12.X/24. O departamento *A* contém três hosts e um servidor ligados a um *switch*, que por sua vez liga ao *router* R_A. O departamento *B* tem três *hosts* ligados a um *hub*, que por sua vez liga ao *router* R_B. Os dois *routers* estão ligados entre si por uma ligação física, cujo endereço de rede é atribuido automaticamente pelo CORE. Todos os *links* têm uma largura de banda de 100 Mbps. Para facilitar a configuração dos endereços de rede, comece por ligar apenas o *switch* e o *hub* aos *routers* e depois configure os endereços IP das interfaces do *router* de acordo com a regra definida. Seguidamente ligue os *hosts* e o servidor ao *switch* e ao *hub*, ficando assim automaticamente configurados com os endereços IP desejados.

No sentido de observar o envio e recepção de mensagens ARP, é conveniente apagar o conteúdo da *cache* ARP. Caso contrario, é provável que a associação entre endereços IP e MAC já exista em *cache*. Apague a *cache* ARP usando o comando *arp –d*. Um método expedito no CORE de apagar todas as caches ARP é reiniciar a rede.

Selecione um *host* dum departamento à sua escolha. Neste *host* inicie a captura de tráfego com o Wireshark do CORE. A partir desse *host* efectue *pings* para **dois** *hosts* localizados na outra rede (departamento). Pare a captura de tráfego no Wireshark e localize o tráfego ARP, usando o filtro *arp*.

8. Abra uma consola no *host* onde efetou o *ping*. Observe o conteúdo da tabela ARP com o comando *arp*.
    a. Com a ajuda do manual arp (*man arp*), interprete o significado de cada uma das colunas da tabela.

    b. Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.

9. Qual é o valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (*ARP Request*)? Como interpreta e justifica o endereço destino usado?

10. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?

11. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? O que conclui?

12. Explicite que tipo de pedido ou pergunta é feita pelo *host* de origem?

13. 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 posição da mensagem ARP está a resposta ao pedido ARP?
    c. A resposta ARP é enviada em *broadcast*? Justifique o modo de envio usado na resposta ARP.

14. Verifique se o *ping* feito ao segundo *host* originou pacotes ARP e justifique a situação observada.

15. Apresente um esquema apenas com as máquinas envolvidas no envio do pedido *ping* desde a origem até ao destino, bem como os endereços IP e MAC das respetivas interfaces de rede, podendo para tal recorrer ao comando *ifconfig*. Represente nesse esquema as tramas com os pedidos e respostas ARP geradas ao longo da rota pelo envio do pedido *ping*. Indique para cada trama os endereços MAC origem e destino presentes no cabeçalho Ethernet, bem como os endereços Sender MAC, Sender IP, Target MAC e Target IP presentes no pacote ARP. Assinale com uma seta o sentido de cada pacote e com um número a ordem de sequência dos pacotes. Considere todas as tabelas ARP vazias no momento em que se fez o *ping*. Ignore a situação da resposta ao pedido *ping.*

5. Domínios de Colisão

Uma rede local onde existam vários equipamentos ligados através de um meio partilhado comum constitui o que é denominado um domínio de colisão. Esta designação decorre da possibilidade de vários *hosts* poderem coincidir temporalmente no envio de uma trama, causando uma interferência mútua (colisão) que deteriora as tramas originalmente enviadas.

Num domínio de colisão, apenas um dispositivo pode transmitir num determinado instante e os restantes ficam à escuta para prevenir colisões. Por esse facto, a largura de banda é partilhada entre os diversos dispositivos. Na presença de uma colisão os dispositivos envolvidos têm que retransmitir a mesma trama Ethernet algum tempo depois. As normas Ethernet implementam um método de controlo de acesso ao meio denominado CSMA/CD (estudado nas aulas teóricas), que prevê a resolução de colisões.

Os domínios de colisão existem em segmentos de rede com equipamentos interligados via *hubs* partilhados (repetidores) e também em redes sem fios (Wi-Fi).

As redes mais modernas usam comutadores de rede (*switches*) para eliminar as colisões. Conectando cada dispositivo a uma porta do comutador, cada porta constitui um domínio de colisão (se a comunicação for *half-duplex*) ou são eliminados se a comunicação for *full-duplex*.

16. Através da opção `tcpdump`, verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando *ping*). Que conclui?

Comente os resultados obtidos quanto à utilização de *hubs* e *switches* no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.

Parte 2: Redes Sem Fios (IEEE 802.11)

1. Estudo Prévio

Antes de iniciar o trabalho, recomenda-se a leitura dos *slides* sobre Redes sem Fios disponíveis na plataforma de ensino, e a consulta do Anexo ao enunciado. Como neste trabalho se aprofundam aspetos da descrição feita nos *slides*, pode-se 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 ,
que é uma versão resumida da norma disponível em:

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

1.1. 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 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.

1.2. Limitações na captura de tráfego WiFi

Como explicado na documentação de apoio do Wireshark, 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 WiFi pode não evidenciar diferenças quando analisadas no Wireshark.

Como o sucesso na captura de tráfego WiFi 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, os alunos podem também realizar capturas de tráfego IEEE 802.11, usando uma de duas abordagens:

(a) via GUI, selecionar *Edit/Preferences/Capture* e, para a interface WiFi (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 wlan0 -I -y IEEE801_11 &`

2. Primeiro Passo

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

3. Acesso Rádio

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 4XX, em que XX corresponde ao seu número de grupo (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. *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 número de grupo, responda às seguintes questões:

4) Selecione a trama *beacon* XX. 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)?

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

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

7) 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. Identifique um *probing request* para o qual tenha havido um *probing response*.

8) Face ao endereçamento usado, indique a que sistemas são endereçadas ambas as tramas e explique qual o propósito das mesmas?

   Sugestão: use a união de filtros *wlan.fc.type_subtype==X* para visualizar no Wireshark todas as tramas *probing request* ou *probing response*, simultaneamente. Para saber o valor do subtipo (X) consulte a tabela do Anexo.

5. 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:

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

10) Efetue um diagrama que ilustre, com as tramas identificadas na alínea anterior, a sequência de todas as tramas trocadas no processo de autenticação e associação entre o STA e o AP.

6. 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.

11) Considere a trama de dados nº 433. 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?

12) Para a trama de dados da alínea anterior, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao *host* sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição.

13) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir, contrariamente ao que acontece numa rede Ethernet.

14) 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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada, identificando a direccionalidade das tramas e os sistemas envolvidos.

Relatório do trabalho

O relatório final deve incluir apenas:

- título e identificação do grupo;

- uma secção "Questões e Respostas" relativas ao enunciado acima (formato: transcrição da questão, resposta, ...);

- uma secção de "Conclusões" que autoavalie (de forma completa) os resultados da aprendizagem decorrentes das várias vertentes estudadas no trabalho.

O relatório deve seguir preferencialmente o formato LNCS (Springer, existem *templates* .tex e .docx) e ser submetido obrigatoriamente em formato pdf na plataforma de ensino com o nome SCR-TP1-GXX.pdf (por exemplo, SCR-TP1-G11.pdf para o grupo G11) até final do dia previsto para a conclusão do trabalho.

Anexo - Trama 802.11 + Tipos e subtipos de tramas

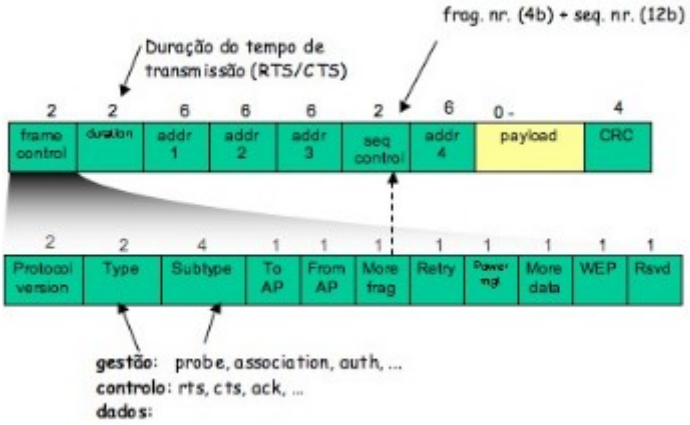


Table 14.4 Valid Type and Subtype Combinations

Type Value	Type Description	Subtype Value	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	1000	Beacon
00	Management	1001	Announcement traffic indication message
00	Management	1010	Dissociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
01	Control	1010	Power save - poll
01	Control	1011	Request to send
01	Control	1100	Clear to send
01	Control	1101	Acknowledgment
01	Control	1110	Contention-free (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 function (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)