Universidade do Minho

Licenciatura em Engenharia Informática

Redes de Computadores

TP2: Camada de Ligação Lógica: Ethernet e Protocolo ARP

(Parte I)

1. Objectivos

O objectivo deste trabalho é estudar, de uma forma genérica, a camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP (*Address Resolution Protocol*).

O protocolo ARP, descrito na RFC 826 (http://tools.ietf.org/html/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. Desta forma, o protocolo ARP permite determinar, por exemplo, qual o endereço Ethernet que corresponde a um endereço IP particular.

2. Introdução

Um dos conceitos mais importantes de uma pilha protocolar estruturada em 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 (PDU) de nível de rede[1] é colocado dentro da 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 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 detecção e recuperação de erros. Estes serviços podem ser oferecidos por outros níveis da pilha protocolar, por exemplo, o nível de transporte com o protocolo TCP[2] . 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.

---

[1] E.g., Datagrama IP

[2] *Transmission Control Protocol*, protocolo de transporte fiável usado na Internet.

Detecção e Correcção de Erros

A detecção e correcção de erros é outro exemplo de uma funcionalidade de serviço que pode ser prestada nos vários níveis da pilha protocolar.

Genericamente a detecção e correcção de erros do nível de ligação lógica, bastante mais sofisticada que nos níveis protocolares superiores, consegue detectar e corrigir erros de um bit e alguns erros com vários bits. O mecanismo detecção mais comum é baseado na criação dum bloco de bits (B) pelo originador, que é uma função *f* da informação presente na trama a ser transmitida. Esse bloco de bits é colocado no cabeçalho da trama. O receptor ao receber a trama, utiliza a mesma função *f* e obtém por seu turno o bloco de bits (B1). Nessa altura, o receptor compara B com B1. Se não forem iguais significa que a trama tem erros e deve ser descartada. Se forem iguais a trama é considerada correta.

Existem diversos métodos de detecção e correcção de erros com menor ou maior complexidade. O método de detecção 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 e WiFi. O WiFi é a designação usada para a ligação em rede local sem fios, usada normalmente como sinónimo da norma IEEE 802.11a/b/g/n.

Protocolos de Acesso de Controlo de Ligação

Há dois tipos de ligações na rede: ligações ponto-a-ponto e ligações de difusão[3]. 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 do mesmo 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 ou redes sem fios (por exemplo Wi-Fi)[4].

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 quase impossível aos receptores receberem correctamente as tramas transmitidas. Assim, o objectivo de um protocolo MAC (*Medium Access Protocol*) é coordenar o acesso ao meio de modo a reduzir a probabilidade ou mesmo eliminar a 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 (taking-*turn*) e protocolos de acesso

[3] *Broadcast*, no original em inglês
[4] *Wireless LAN*

aleatório. Em particular, estes últimos são de extrema importância nas redes locais.

Endereços MAC

A nível de ligação lógica, e em particular nas redes LAN, 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 emissor muda de rede. Daí ser também designado como endereço físico. Pelo contrário, um endereço IP é um endereço lógico, i.e. muda consoante a 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 rede que interliga.

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 WiFi, todos os nós da rede local recebem a trama. Cada nó receptor 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 excepção: se o endereço destino for FF-FF-FF-FF-FF-FF (endereço de difusão) todos os nós recebem e processam a trama.

Address Resolution Protocol

O principal objectivo 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.

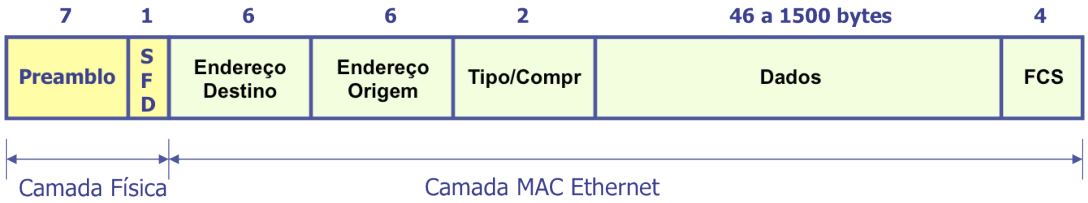
Suponha que um host na rede local quer enviar um datagrama IP para outro host na rede local. Suponha que conhece, provavelmente a partir do serviço de resolução de nomes – DNS, o endereço IP do host destino. Como sabe, o datagrama IP para ser enviado terá de ser entregue à camada de ligação lógica (L2) 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 fonte 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.

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 (10Mbps a 10Gbps). A tecnologia Ethernet implementa um método de controlo de acesso ao meio que será estudado nas aulas teóricas, e usa um formato de trama simples que inclui campos de controlo e um campo de dados.

Um trama Ethernet tem exactamente seis campos: (i) um campo para uma sequência de bits específica chamado *preâmbulo* (que o host destino utiliza para sincronizar o seu relógio com o relógio do host de origem e, assim, determinar quando começa a trama); (ii) endereço MAC destino; (iii) endereço MAC origem; (iv) um campo que indica 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 detecção de erros (CRC-32).



Interligação de Redes Locais

As redes locais são interligadas através de *hubs*, *bridges* ou *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* são dispositivos do nível de ligação lógica, processando tramas do nível de ligação. Um *switch,* com a ajuda duma 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 dum mecanismo de auto-aprendizagem. Quando chega uma trama a uma das suas interfaces, o *switch* examina o endereço fonte da trama e acrescenta uma entrada na tabela com o endereço MAC correspondente. Finalmente, quando chega uma trama que o *switch* não consegue encaminhar com base na tabela de comutação faz uma difusão através de todas as suas interfaces.

Por sua vez os *routers*, que serão estudados em detalhe mais adiante, lidam com os endereços IP dos datagramas de maneira parecida como os *switches* lidam com os tramas. Para esse efeito utilizam uma tabela de encaminhamento que é preenchida quer manualmente com rotas estáticas ou automaticamente através da utilização de protocolos de encaminhamento como o OSPF.

As entradas da tabela 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 e análise de tramas Ethernet será efectuada usando o Wireshark.

Assegure-se que a *cache* do seu browser está vazia.

Arranque o Wireshark na sua máquina nativa.

No seu browser, aceda ao seguinte URL `http://marco.uminho.pt/CCG/`, correspondente à página de apresentação do Grupo de Comunicações por Computador.

Pare a captura do Wireshark.

Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à mensagem `HTTP GET` enviada pelo seu computador para o servidor Web no sistema `marco.uminho.pt`, bem como o começo da respectiva mensagem `HTTP Response` proveniente do servidor.

Nesta fase, como se pretende estudar apenas o nível de ligação lógica pode eliminar informação sobre o nível IP e níveis superiores, desabilitando os protocolos IPv4 e IPv6.

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 de uma trama Ethernet. Expanda a informação Ethernet II 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 possível, quando responder a uma questão, deve usar a impressão do pacote na captura que precisa para responder à questão colocada. Para imprimir um pacote, use File-→Print, escolha *Selected packet only* e *Packet summary line.* Selecione o mínimo detalhe necessário para responder à pergunta.

1. Qual é o endereço MAC da interface ativa do seu computador?
2. Qual é o endereço MAC destino da trama? Em sua opinião, a que sistema é destinada essa trama, ou dito de outra forma, será destinada ao endereço Ethernet do servidor `marco.uminho.pt`? Justifique.
3. Qual o valor hexadecimal presente no campo tipo (`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? Tente obter uma indicação do *overhead* introduzido pela pilha protocolar.
5. Qual é o valor hexadecimal do campo FCS na trama capturada (poderá não estar a ser utilizado)?

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

6. Qual é o endereço Ethernet da fonte? É o endereço do seu computador ou do servidor `marco.uminho.pt`? Qual o dispositivo que enviou a trama?
7. Qual é o endereço MAC do destino? Reconhece-o?
8. Qual o valor hexadecimal do campo tipo (`Type`)?
9. Quantos *bytes* contém a trama Ethernet antes do caractere ASCII corresponde ao 200 OK (isto é o código de resposta do HTTP)?
10. Qual é o valor hexadecimal do campo FCS da trama Ethernet?

4. Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP.

11. Verifique o conteúdo da *cache* ARP do seu computador.

- **MS-DOS.** Digite `arp ou c:\windows\system32\arp` na linha de comando.
- **Linux/Unix**. O executável para o comando `arp` pode estar em vários locais. É habitual estar em `/sbin/arp` (Linux), `/usr/sbin/arp` ou `/usr/etc/arp` (para outras variantes de Unix). O comando `arp` sem argumentos ou com a opção `-a` mostra o conteúdo da *cache* do seu computador (ver detalhes em `man arp`).

12. Observe o conteúdo da tabela ARP. O que significa cada uma das colunas?

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*.

- **MS-DOS.** O comando MS-DOS `arp -d *` apaga a *cache* ARP. A flag –d indica a operação de remoção e o * (*wildcard*) indica que a operação é feita para todas as entradas da tabela.
- **Linux/Unix.** O comando `arp -d *` apaga a *cache* ARP. Este comando necessita de privilégios de `root`).

Para observar o protocolo ARP em operação, apague novamente a *cache* ARP e assegure-se que o *cache* do browser está vazia.

Inicie a captura de tráfego com o Wireshark, e aceda a http://marco.uminho.pt. Pode simultaneamente tentar efectuar *ping* para um host da sala de aula.
Pare a captura de tráfego e tente localizar o tráfego ARP.

Se for necessário, limite a lista de protocolos do Wireshark apenas a protocolos abaixo do nível IP. Para tal, seleccione *Analyze->Enabled Protocols* e remova a selecção da opção IPv4 e IPv6.

Responda às seguintes perguntas:

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

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

15. Qual o valor do campo ARP *opcode*? O que especifica? Se necessário, consulte a RFC do protocolo ARP http://tools.ietf.org/html/rfc826.html.

16. A mensagem ARP contém o endereço IP do originador? Que tipo de pergunta é feita?

17. Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.
    a. Qual o valor do campo ARP *opcode*? O que especifica?
    b. Em que posição da mensagem ARP está a informação que responde ao pedido ARP?

18. Quais são os valores hexadecimais para os endereços fonte e destino da trama que contém a resposta ARP? Que conclui?

5. ARP numa topologia CORE

No emulador CORE prepare uma topologia com três *routers* em que n1 liga a n2 e este a n3.

19. Com auxílio do `ifconfig` obtenha os endereços Ethernet das interfaces dos diversos *routers*.

20. Usando o comando `arp` obtenha o conteúdo das *caches* `arp` dos diversos sistemas.

21. Faça `ping` de n1 para n2. Que modificações observa nas *caches* ARP dos sistemas envolvidos.

22. Faça `ping` de n1 para n3. Consulte as caches ARP. Que conclui?

23. Em n1 remova a entrada correspondente a n2. Coloque uma nova entrada para n2 com endereço Ethernet errado. O que acontece?

Adicione agora um *switch* (n4) à topologia e lige o *router* n1, e os *hosts* n5 e n6 a esse *switch*.

24. Faça `ping` de n5 para n6. Sem consultar a tabela ARP anote a entrada que, em sua opinião, é criada na tabela ARP de n5. Verifique se a sua interpretação sobre a operação da rede Ethernet e protocolo ARP estava correto.

(Fim da Parte I)