E-fólio B | Instruções para a realização do E-fólio

SISTEMAS EM REDE | 21106

UNIDADE CURRICULAR: **Sistemas em Rede**

CÓDIGO: **21106**

DOCENTE: **Arnaldo Santos e Henrique São Mamede**

A preencher pelo estudante

NOME: Pedro Nuno Esteves de Abreu

N.º DE ESTUDANTE: 2300485

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 19-12-2025

TRABALHO / RESOLUÇÃO:

Questão 1: Funcionamento do Protocolo ARP

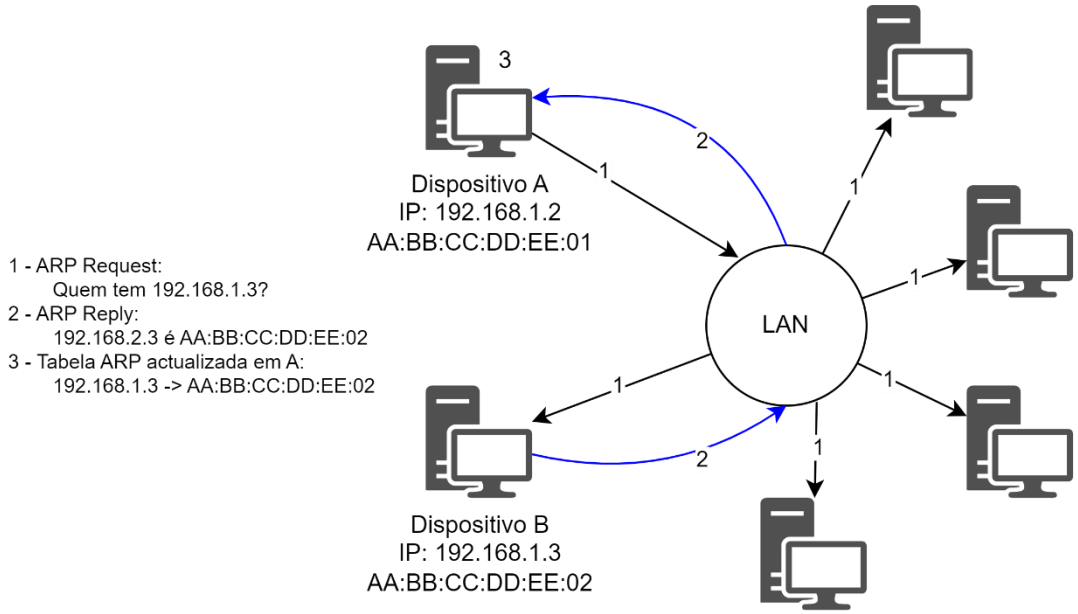
Obectivo:

O **ARP (Address Resolution Protocol)** permite mapear endereços IP (camada de rede) em endereços MAC (camada de enlace de dados), conforme modelo de OSI. O protocolo ARP é essencial em redes TCP/IP para:

1. **Mapear IPs em MACs**: Garante que dispositivos na mesma rede possam comunicar-se, mesmo que apenas os endereços IP sejam conhecidos.
2. **Facilitar a comunicação local**: O ARP resolve automaticamente a associação entre IP e MAC, permitindo a entrega correcta dos pacotes na camada de enlace.
3. **Eficiência**: O uso da **tabela ARP** (cache) optimiza o desempenho, armazenando temporariamente as associações já resolvidas.

Funcionamento:

- Quando um dispositivo precisa comunicar com outro dispositivo numa rede, envia um **ARP Request** em **broadcast** para todos os dispositivos da rede através dessa mesma rede (na imagem pressupõe-se uma LAN).
- O dispositivo que possui o IP solicitado responde com um **ARP Reply** (Unicast), através da rede, informando o seu endereço MAC.
- A tabela ARP armazena temporariamente o mapeamento entre os IPs e os endereços MAC.



Formato de uma mensagem ARP:

O cabeçalho ARP contém os seguintes campos principais:

- **Hardware Type**: Tipo de hardware (exemplo: Ethernet).
- **Protocol Type**: Tipo de protocolo da camada superior (exemplo: IPv4).
- **Hardware Address Length** e **Protocol Address Length**: Comprimentos dos endereços MAC e IP.
- **Operation**: Tipo de operação (Request ou Reply).

- **Endereços de Origem/Destino**: Contém os endereços MAC e IP dos dispositivos.

Hardware Type	Protocol Type	Hardware Adress Length	Protocol Address Length	Operation	Origin Adress	Destiny Adress
1 (Ethernet)	0x0800 (IPv4)	6 (tamanho do MAC)	4 (tamanho do IPv4)	1 (Request)	192.168.1.2 AA:BB:CC:DD:EE:01	192.168.1.3 00:00:00:00:00:00
1 (Ethernet)	0x0800 (IPv4)	6 (tamanho do MAC)	4 (tamanho do IPv4)	2 (Reply)	192.168.1.3 AA:BB:CC:DD:EE:02	192.168.1.3 AA:BB:CC:DD:EE:01

Cabeçalhos do exemplo acima (ver funcionamento). Note-se que, no Request, o endereço de destino o MAC é desconhecido, já que é precisamente o que se pretende saber. No Reply o endereço de destino já vai preenchido (é sabido quem fez a pergunta) e por isso pode ser enviado em Unicast. Referência RFC 826.

Tipos de ARP:

- **Gratuitous ARP**: Um dispositivo anuncia o seu endereço IP na rede, sem que ninguém tenha solicitado. Isso é usado para evitar conflitos de IP.
- **RARP (Reverse ARP)**: Resolve o endereço IP a partir do endereço MAC, geralmente utilizado por dispositivos sem configuração prévia.
- **ARP Spoofing/Poisoning**: Técnica maliciosa usada para alterar a tabela ARP de um dispositivo, redireccionando o tráfego.

Proxy ARP:

Quando o emissor e o destinatário estão em redes diferentes, um **roteador** pode responder ao ARP Request com o seu próprio endereço MAC, assumindo a responsabilidade de encaminhar os pacotes para o destino.

Usos comuns

- **Comunicação Local (LAN)**:
  Dois dispositivos na mesma rede utilizam o ARP para descobrir o endereço MAC um do outro.
- **Comunicação Entre Redes (Router)**:
  Quando um dispositivo precisa comunicar com outra rede, envia o pacote ao **router**. O ARP resolve o endereço MAC do **gateway**.
- **ARP Cache**:
  As informações obtidas pelo ARP são armazenadas temporariamente na **tabela ARP (cache)**. Isto evita que a rede seja inundada por mensagens ARP repetidas.

Curiosidade: ao ler o RFC 826 não reparei logo que era de 1982. Quando li sobre a motivação da sua criação se falava no crescente uso da ethernet a 10Mbit fiquei baralhado e então fui mais acima e reparei que o texto (com actualizações) já tem 43 anos.

Também a título de curiosidade, se quisermos conhecer a tabela ARP do nosso PC basta executar na linha de comandos **arp -a**. Serão mostradas as entradas da tabela.

Referências: Tanenbaum & Wetheral, 2011, págs 467-469; RFC 826

Questão 2: Estrutura de uma Frame Ethernet (802.3 Standard)

Obectivo:

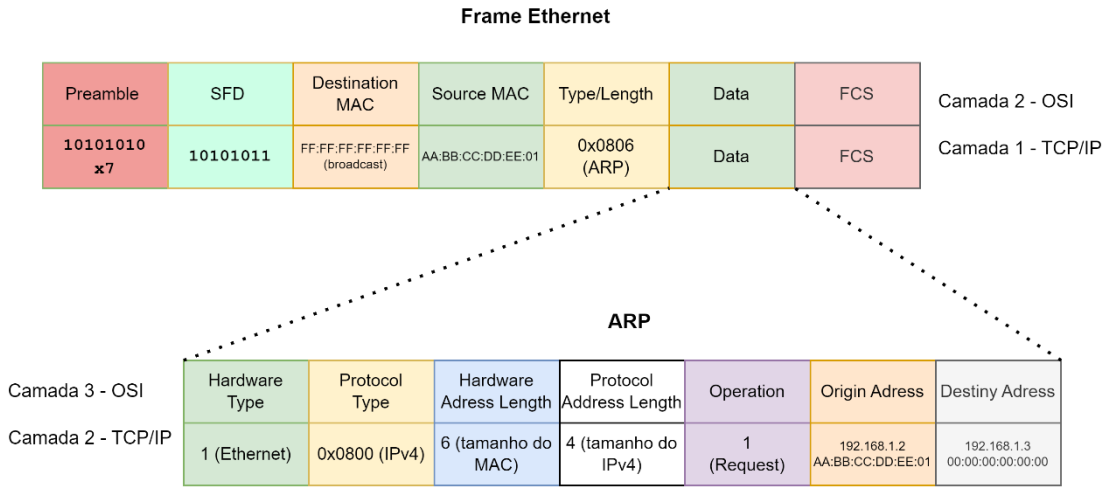
A Frame Ethernet é a unidade de dados de transmissão na camada de enlace da **rede Ethernet**.

Formato (estrutura) de uma Frame Ethernet (IEEE 802.3)

A estrutura de uma Frame Ethernet inclui os seguintes campos:

- **Preamble (7 Bytes):**
  - Sequência de 10101010 repetida.
  - Utilizada para sincronização entre o transmissor e o receptor.
- **Start of Frame Delimiter (SFD) (1 Byte):**
  - Finaliza a sincronização com 10101011.
  - Indica que a frame está prestes a começar.
- **Destination MAC Address (6 Bytes):**
  - Endereço físico do destinatário.
  - Pode ser unicast, broadcast (FF:FF:FF:FF:FF:FF) ou multicast.
- **Source MAC Address (6 Bytes):**
  - Endereço físico do remetente da frame.
- **Type/Length (2 Bytes):**
  - Se o valor é ≤ 1500: indica o tamanho do campo de dados.
  - Se o valor é ≥ 1536 (0x0600): identifica o protocolo de camada superior (ex.: IPv4 → 0x0800).
- **Data/Payload (46-1500 Bytes):**
  - Contém os dados da camada superior (ex.: pacote IP).
  - Caso o tamanho dos dados seja inferior a 46 bytes, é adicionado padding para atingir o tamanho mínimo da frame (64 bytes).
- **Frame Check Sequence (FCS) (4 Bytes):**
  - Usa CRC (Cyclic Redundancy Check) para detetar erros na transmissão.
  - Se a verificação falhar, a frame é descartada.

A Frame Ethernet clássica (1978) tinha uma pequena diferença para a Frame Ethernet IEEE 802.3 (1983): o preâmbulo era formado por 8 bytes, ou seja, incluía o byte que na IEEE 802.3 corresponde ao Start of Frame Delimiter (SoF ou SFD). (. (Tanenbaum & Wetheral, 2011, págs 281-282)



Cabeçalhos do broadcast exemplificado na questão 1 deste e-fólio. Colocado apenas por curiosidade, para destacar a relação entre o ARP e a Frame Ethernet. Também para realçar que pertencem a camadas diferentes e fazer a ligação com a questão 1 do e-fólio A.

Referências: Tanenbaum & Wetheral, 2011, págs 282-285

Questão 3: Definição e Comparação LAN vs WAN

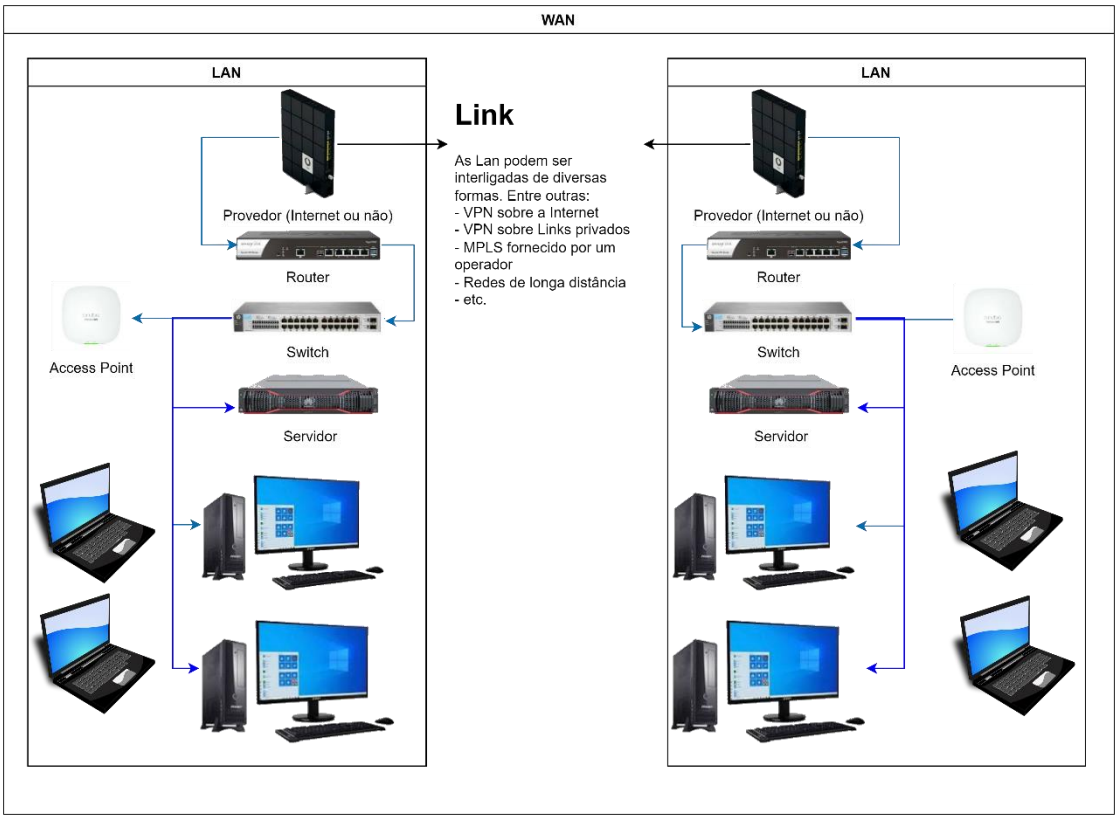
A LAN (Local Area Network) pode ser definida como sendo “uma rede privada projetada para operar dentro de uma área geográfica limitada, como uma casa, escritório ou escola, usada principalmente para ligar computadores pessoais e dispositivos eletrónicos.” (Tanenbaum & Wetheral, 2011, pág 19). Pode-se acrescentar que as LAN’s permitem que os dispositivos comuniquem entre si e compartilhem recursos como arquivos, impressoras e ligações de Internet de forma eficiente (phoenixNAP). Uma LAN, que era tradicionalmente ligada por cabo, pode ser, de há uns anos a esta parte, também ligada por WiFi.

Já uma WAN (Wide Area Network) é uma rede que abrange uma grande área geográfica, frequentemente um país ou continente, ligando múltiplos escritórios ou instalações em diferentes localidades [Tanenbaum & Wetheral, 2011, págs 23-24]. As WAN são utilizadas para ligar LAN’s e essas ligações podem ser de vários tipos [phoenixNAP]:

- Linha Contratada WAN:
  - Utiliza circuitos dedicados privados para ligar locais.
  - Ideal para alta confiabilidade e baixa latência.
  - Usada para aplicações críticas que exigem largura de banda consistente.
- WAN Comutada por Circuito:
  - Estabelece uma comunicação dedicada durante a ligação.
  - Exemplo: Redes telefônicas tradicionais.
  - Confiável, mas ineficiente para transmissão de dados em comparação com outras opções.
- WAN Comutada por Pacotes:
  - Dados são divididos em pacotes e enviados por uma rede compartilhada.
  - Exemplos: Frame Relay, X.25, e redes baseadas em IP.
  - Eficiente e económica, optimiza a largura de banda.

- PSTN (Rede Telefônica Pública Comutada):
    - Criada originalmente para voz, mas também usada para transmissão de dados via modems.
    - Limitada a dados de baixa velocidade, mas ainda útil em áreas remotas.
- RDIS (Rede Digital de Serviços Integrados):
    - Transmite voz, vídeo e dados por linhas telefónicas tradicionais.
    - Oferece melhor qualidade e velocidade que ligações dial-up.
    - Ideal para aplicações como videoconferências.
- ATM (Modo de Transferência Assíncrona):
    - Rede de alta velocidade para dados, voz e vídeo.
    - Utiliza células de tamanho fixo para desempenho previsível.
    - Limitada pela complexidade e alto custo.
- MPLS (Comutação de Rótulo Multiprotocolo):
    - Direciona dados com base em rótulos em vez de endereços longos.
    - Oferece alta eficiência e suporte a múltiplos tipos de tráfego.
    - Amplamente usado para criar VPNs privadas.
- SD-WAN (Rede de Área Ampla Definida por Software):
    - Gere ligações WAN usando tecnologias baseadas em software.
    - Combina múltiplos tipos de ligações (banda larga, LTE, MPLS).
    - Proporciona melhor desempenho, redução de custos e maior flexibilidade.

Diagrama de Interligação LAN e WAN:



Vantagens de uma LAN Sem Fios (Wireless):

1. **Mobilidade e Flexibilidade**:
    - Permite que os utilizadores se liguem à rede sem depender de cabos, proporcionando maior liberdade de movimento.
    - Ideal para dispositivos móveis (laptops, smartphones, tablets) e áreas de trabalho dinâmicas. Mas, hoje em dia, os PCs podem ter antenas, e grande parte das impressoras também têm a vertente Wifi.
2. **Facilidade de Instalação**:
    - Não requer infraestrutura física extensa (cabos e switches), reduzindo custos iniciais e tempo de instalação, especialmente em edifícios ou locais onde a instalação de cabos é difícil.

Desvantagens de uma LAN Sem Fios (Wireless):

1. **Velocidade e Latência Inferiores**:
    - Redes sem fios oferecem menor velocidade de transmissão de dados e maior latência em comparação com redes com fios (especialmente fibra ótica).
    - Sofre mais com interferências e congestionamento.
2. **Segurança**:
    - É mais suscetível a ataques, como **interceptação de dados** e acessos não autorizados, especialmente se as medidas de segurança (ex.: WPA3) não forem implementadas adequadamente.
    - Redes com fios oferecem maior controle físico e proteção contra invasões externas.

Questão 4:

a) Algoritmo de Inundação (Flooding)

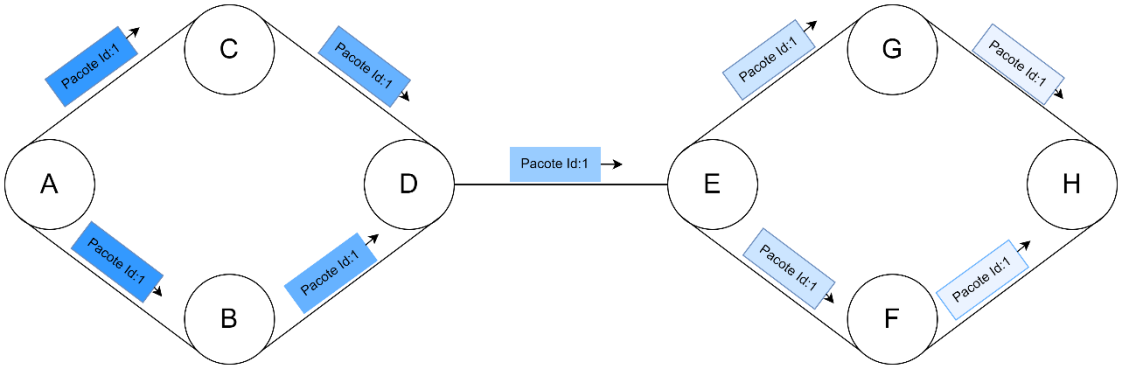
O algoritmo de Inundação (Flooding) é um método de roteamento estático onde os pacotes são enviados através de todas as ligações disponíveis numa rede (excepto a origem do mesmo) até atingirem o destino [Tanenbaum & Wetheral, 2011, págs 368-24].

Funcionamento do Algoritmo de Flooding

1. **Envio Inicial**:
    - Quando um nó (router) recebe um pacote, envia-o por **todas as suas ligações (links)** excepto pelo link de onde o pacote foi recebido.
    - Este processo garante que todos os nós ligados na rede recebam o pacote.
2. **Multiplicação de Pacotes**:
    - O pacote é replicado para cada saída disponível, criando várias cópias ao longo da rede.

- Isso pode levar a uma **sobreposição de pacotes**, aumentando o tráfego na rede.

3. **Mecanismos de Controle**: Para evitar problemas como loops infinitos ou sobrecarga, são utilizados controles, como:
   - **Time-to-Live (TTL)**:
     - Cada pacote contém um contador de hops chamado **TTL**, que é decrementado em cada nó.
     - Quando o TTL atinge **0**, o pacote é descartado.
   - **Detecção de Pacotes Duplicados**:
     - Cada pacote possui um **identificador único**. Os roteadores mantêm um registo dos pacotes já recebidos para evitar reenviar pacotes duplicados.
4. **Entrega ao Destino**:
   - Assim que o pacote chega ao nó de destino, o processo termina.



No caso prático:

Se o router A quer enviar um pacote ao router F, envia-o a todas as suas ligações (routers B e C), estes, por sua vez, ao receberem o pacote, reenviam-no para as suas ligações (excepto o router A, que foi de onde o receberam). Ou seja, tanto B como C enviam o pacote para D. Este router descarta um dos pacotes, pois é duplicado e reenvia o outro para E (de B e C recebeu, por isso não reenvia). O processo é replicado a partir de E até chegar a H se a contagem de hops ainda não tiver chegado a zero antes.

O algoritmo de inundação tem vantagens:

- Garante que o pacote chega ao destino, desde que exista um caminho válido;
- É simples de implementar.

Por outro lado, tem também desvantagens:

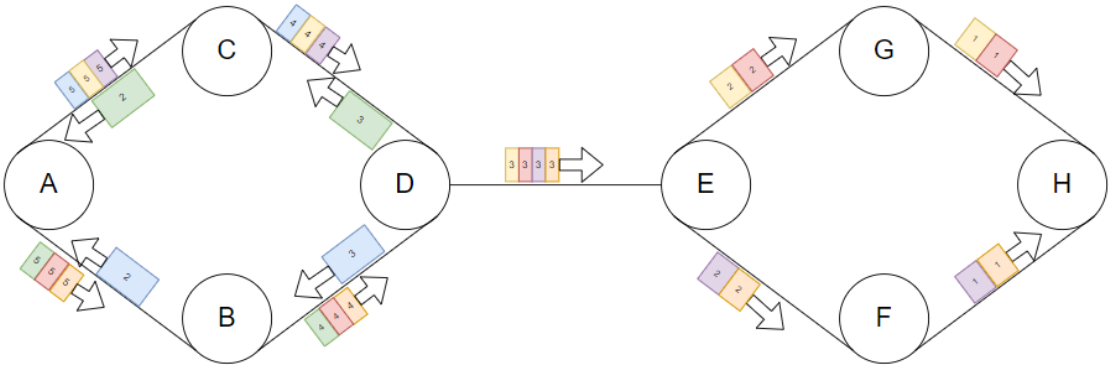
- Pode sobrecarregar a rede com pacotes duplicados, consumindo largura de banda e processamento

b) Rotas

Vejo 3 regras para se determinar as rotas:

- O pacote segue enquanto 'tiver hops';
- O pacote é distribuído para todas as ligações execpto para aquela de onde foi recebido:
- Quem já recebeu ignora.

Se igornarmos a última regra poderemos dizer que, em teoria, existem 6 rotas possíveis para o pacote:



Rota 1: A → C → D → B → A

Rota 2: A → B → D → C → A

Rota 3: A → C → D → E → G → H

Rota 4: A → C → D → E → F → H

Rota 5: A → B → D → E → G → H

Rota 6: A → B → D → E → F → H

As rotas que permitem que o pacote chegue ao destino são as rotas 3, 4, 5 e 6.

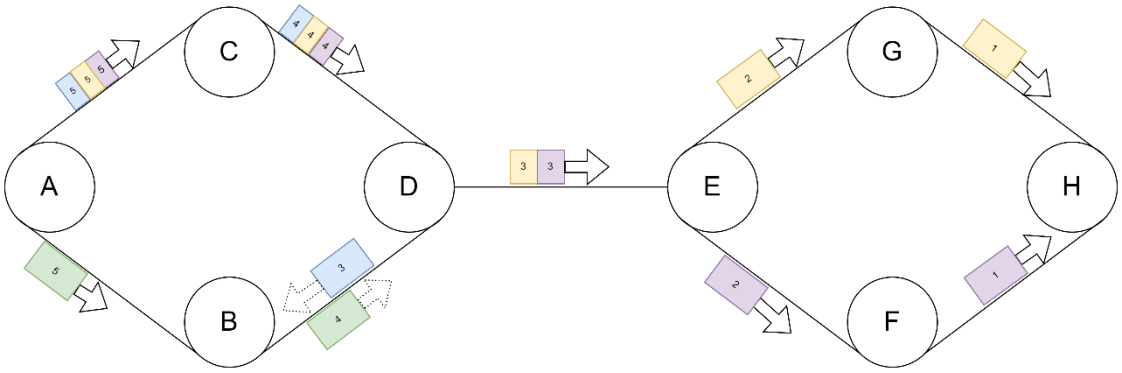
As rotas 1 e 2 não permitem chegar ao destino porque ambas voltam a A.

Isto é, no fundo, em parte o objectivo do flooding: se por qualquer razão uma rota for interrompida (router em baixo, por exemplo), há sempre (ou quase sempre) uma forma de o pacote chegar ao destino.

Contudo, na prática, e dado que o pacote é enviado por A para B e C ao mesmo tempo, poderá haver lugar à aplicação da regra em que quem já recebeu o pacote ignora novas recepções (ou melhor não o envia de novo). Nesse caso algumas das rotas não são possíveis 'ao mesmo

tempo'. No caso concreto, o pacote que vai de D para E ou vem de C ou vem de B. Só sairá um, pois D ignorará aquele que chegar depois.

Assim o fluxo das rotas seria o seguinte. No fluxo parto do princípio de que os tempos de envio são diferentes entre os routers. Ou seja, que por A->C->D o tempo não é exactamente o mesmo que por A->B->D. Vou considerar o primeiro mais rápido.



Rota 1: A → C → D → B (se D receber de C antes de receber, pela rota 2, de B)

Rota 2: A → B → D (se B receber de A antes de receber, pela rota 1, de D)

Rota 3: A → C → D → E → G → H

Rota 4: A → C → D → E → F → H

As rotas que permitem que o pacote chegue ao destino são as rotas 3 e 4.

As rotas 1 e 2 não permitem chegar ao destino porque:

- A rota 1 acaba em B porque este router já recebeu o pacote de A e, portanto, ignora-o;
- A rota 2 acaba em D porque este router já recebeu o pacote de C e, portanto, ignora-o.

Nota:

Se considerarmos que o pacote chega exactamente ao mesmo tempo pela rota 1 (azul) e 2 (verde), então o pacote será enviado apenas para E e a rota 1 termina em D.

Hops consumidos por todas as rotas

- Rota 1: 3 hops.
- Rota 2: 2 hops.
- Rota 3: 5 hops.
- Rota 4: 5 hops.

Total de hops consumidos: 3 + 2 + 5 + 5 = 15 hops.

Referências

Tanenbaum, Andrews, & Wetheral, David. 2011. Computer Networks (5.ª ed), Prentice Hall

RFC 826, RFC Editor, 1982
https://www.rfc-editor.org/rfc/rfc826

phoenixNAP, Glossário de TI
https://phoenixnap.pt/gloss%C3%A1rio/

Fluxogramas desenhados com drawio-desktop v25.0.2