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

UNIDADE CURRICULAR: **Sistemas em Rede**

CÓDIGO: **21106**

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

NOME:

N.º DE ESTUDANTE:

CURSO: Licenciatura em Engenharia Informática

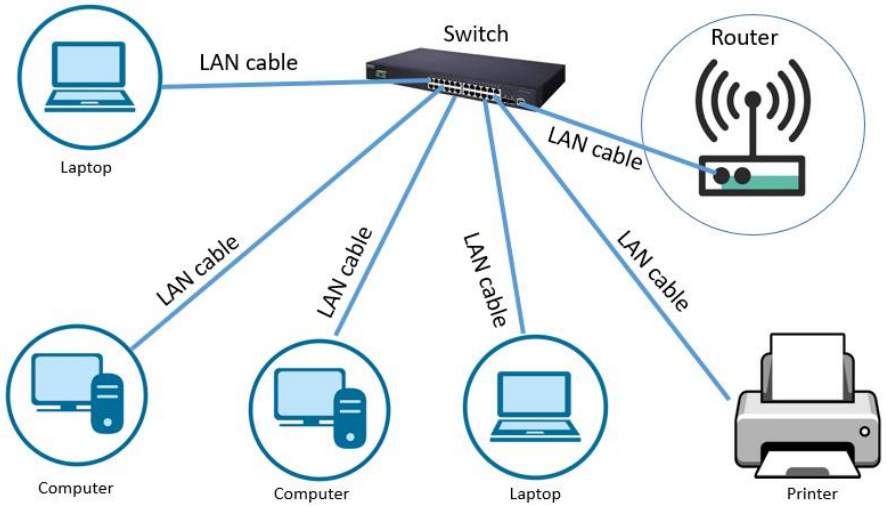
DATA DE ENTREGA: 21 de dezembro de 2025

TRABALHO / RESOLUÇÃO:

1 – Uma LAN (*Local Area Network*) é uma rede de dados que cobre uma área geográfica limitada (por exemplo: uma sala, um piso, um edifício ou um campus), tipicamente sob administração de uma única entidade ou organização, usando tecnologias de acesso locais como Ethernet (IEEE 802.3) e/ou Wi-Fi (IEEE 802.11). Em geral, caracteriza-se por elevadas taxas de transmissão, baixa latência e custos de operação por utilizador relativamente baixos, quando comparada com redes de maior escala (Tanenbaum, 2013).

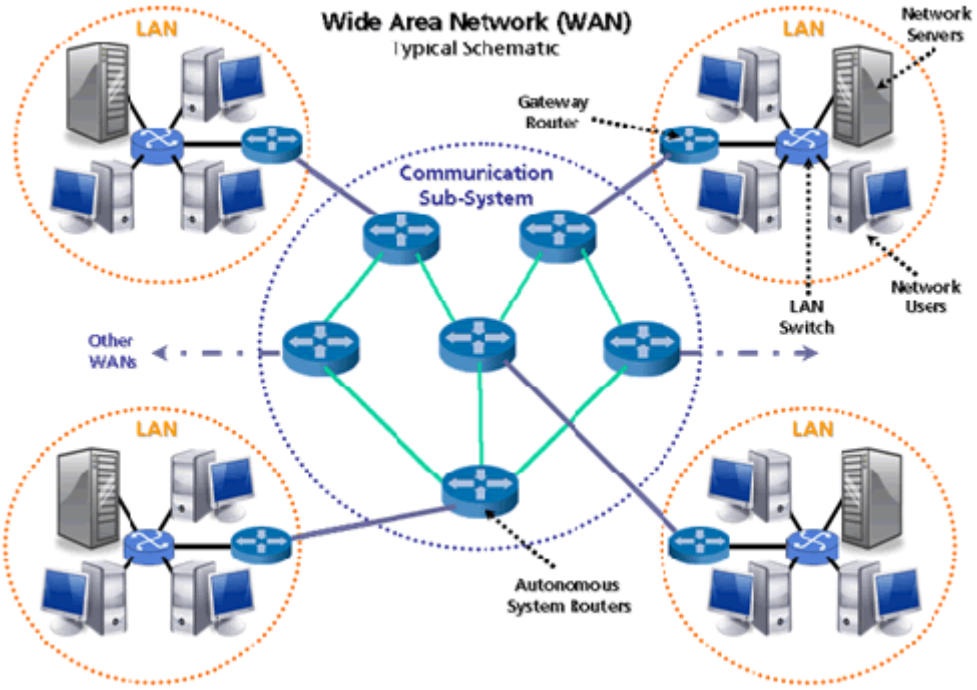
Uma WAN (*Wide Area Network*) é uma rede que interliga LAN (e outras redes) ao longo de uma grande área geográfica (cidades, países, continentes ou vários continentes). A infraestrutura e ligações de uma WAN são frequentemente providenciados por operadores de telecomunicações/*Internet Service Providers*, podendo recorrer a diferentes meios e tecnologias de transporte (por exemplo, fibra ótica, rádio/micro-ondas, cabos submarinos e ligações satélite, entre outros). Em comparação com LAN, tende a ter maior latência, gestão mais complexa e dependência de operadores de telecomunicações (Tanenbaum, 2013).

A figura seguinte demonstra um exemplo de uma LAN doméstica ou de um pequeno escritório, onde vários dispositivos (PC, portátil, impressora) comunicam através de um *switch* e/ou *router*.



Retirado de https://itrelease.com/2021/04/what-is-local-area-network-lan-in-computer/

A figura abaixo apresenta várias LANs (à volta) ligadas por uma rede de transporte no centro (a WAN), composta por routers que encaminham pacotes entre locais distantes.



Retirado de https://marrciohenrique.wordpress.com/2014/03/22/tipos-de-redes-wan-lan-man/

2 – Uma WLAN (*Wireless Local Area Network*) é uma rede local (LAN) em que a ligação entre os dispositivos e a infraestrutura de rede é feita sem cabos, usando ondas de rádio, tipicamente segundo o padrão IEEE 802.11 (Wi-Fi), através de pontos de acesso (*Access Points*) que ligam os clientes sem fios à rede local e ao resto da infraestrutura (Tanenbaum, 2013).

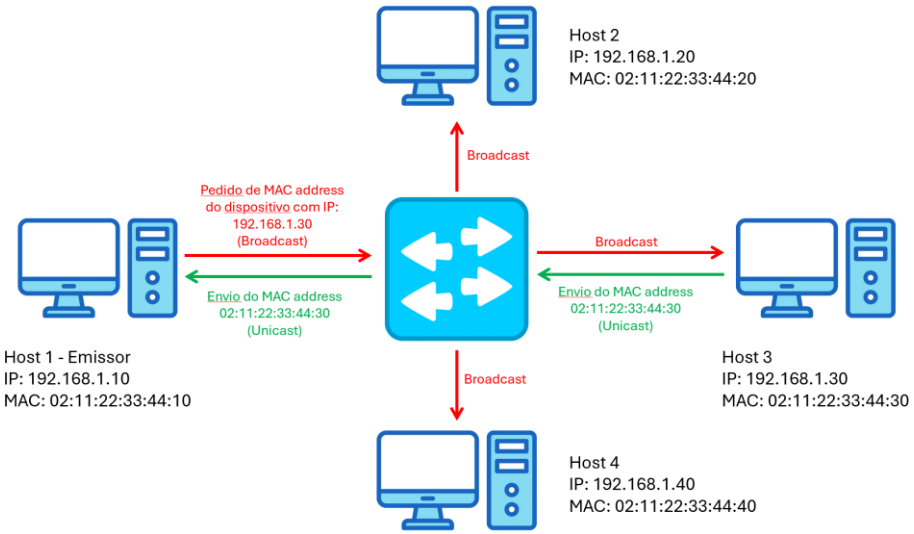
Comparativamente com uma LAN com fios, a WLAN tem as seguintes vantagens (Kurose, 2021; Tanenbaum, 2013):

- Garante uma maior mobilidade e flexibilidade, permitindo que os utilizadores desloquem dentro da área de cobertura mantendo conectividade, sem depender de tomadas/rede cablada;
- Facilidade de instalação e expansão, pois em muitos cenários é mais simples/rápido adicionar utilizadores ou cobrir novas áreas, evitando passagem de cabos.

Por outro lado, a WLAN apresenta as seguintes desvantagens face a uma LAN com fios (Kurose, 2021; Tanenbaum, 2013):

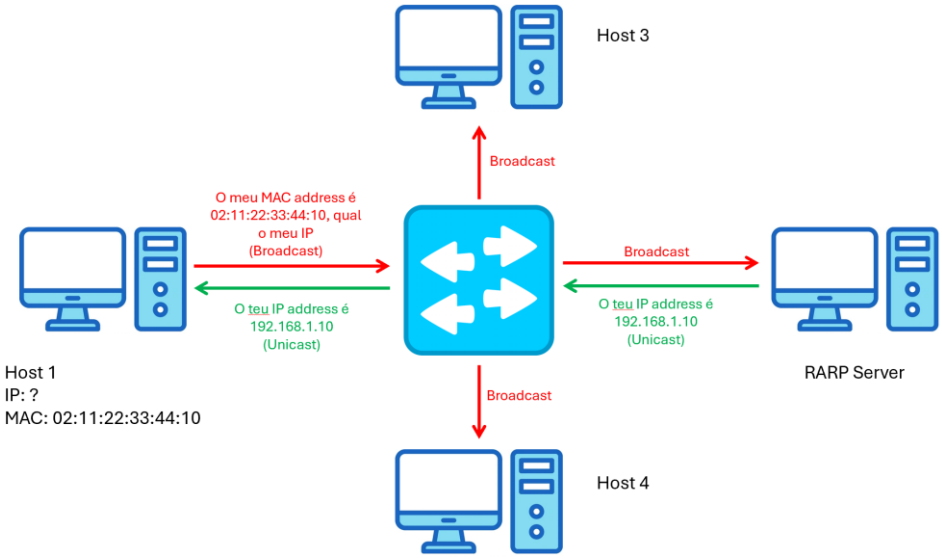
- Menor desempenho e maior variabilidade, uma vez que a taxa efetiva e a latência tendem a ser piores e mais instáveis devido a partilha do meio, distância, obstáculos e interferências;
- Maior exposição a riscos de segurança, pois o sinal propaga-se no espaço físico, o que aumenta a superfície de ataque, pelo que exige uma configuração cuidada para reduzir intrusões e escutas.

3 – O ARP (Address Resolution Protocol) é um protocolo utilizado para resolver ou mapear endereços IP em endereços físicos (MAC) numa rede local baseada em Ethernet. A sua finalidade é permitir que um nó, sabendo o IP de destino (ou o IP do *gateway*), obtenha o MAC necessário para encapsular o datagrama IP numa *frame* Ethernet e o entregar no mesmo domínio de difusão (*broadcast domain*). O funcionamento é, em termos gerais, o seguinte: o emissor consulta a cache ARP; caso não exista correspondência, emite um ARP *Request* em *broadcast* perguntando quem possui determinado IP; o nó que detém esse IP responde com um ARP *Reply* em *unicast*, indicando o seu MAC; a entrada é registada na cache e o tráfego IP pode então ser enviado encapsulado para esse MAC. Importa notar que, quando o destino está fora da sub-rede local, o *host* não resolve o MAC do destino final, mas sim o MAC do router (*default gateway*), para o qual encaminha o datagrama (Tanenbaum, 2013). A imagem seguinte apresenta este funcionamento.



O RARP (*Reverse Address Resolution Protocol*), oi concebido para resolver o problema inverso ao ARP, ou seja, permitir que um equipamento conheça o seu endereço IP a partir do seu endereço MAC, sendo historicamente relevante

em cenários de arranque de máquinas sem disco. O procedimento RARP consiste em o cliente emitir um RARP *Request* em *broadcast* contendo o seu MAC, um servidor RARP que tenha uma tabela de correspondência MAC-IP, responde com um RARP *Reply*, atribuindo/indicando o IP ao cliente (Tanenbaum, 2013). Este procedimento encontra-se esquematizado na figura abaixo.



De referir que, tal como o ARP, o RARP opera no âmbito da rede local e não é encaminhado por routers. Em termos práticos, o RARP é atualmente obsoleto, tendo sido substituído por mecanismos mais completos, como o DHCP, que suportam configuração adicional (*gateway*, DNS, tempo de concessão, etc.).

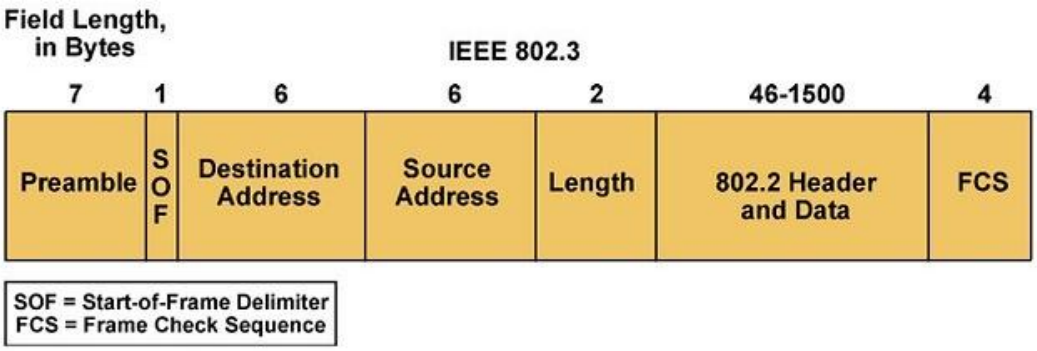
4 – O *Network Provisioning*, ou dimensionamento de capacidade da rede, é uma abordagem preventiva de gestão de congestionamento que consiste em planear e alocar recursos suficientes (largura de banda, capacidade de interfaces, buffers e, em geral, capacidade de encaminhamento) para que, mesmo em períodos previsíveis de pico, a carga oferecida não exceda a capacidade disponível. Ou seja, se houver um sobredimensionamento da rede, *overprovisioning*, nas ligações e nos equipamentos críticos, a probabilidade de filas longas, perdas e aumento de atraso diminui, reduzindo a ocorrência de congestionamento (Tanenbaum, 2013). O *Provisioning* apresenta as seguintes limitações:

- Custo e subutilização – Garantir esta “sobre-capacidade” implica investimento (links mais rápidos, equipamentos mais caros) e pode resultar em capacidade subaproveitada durante grande parte do tempo;

- Não resolve picos súbitos/imprevisíveis – Em casos de tráfego explosivo (eventos, falhas, ataques) pode exceder rapidamente a capacidade prevista;
- Não garante justiça ou *Quality of Service* por aplicação – Sem mecanismos adicionais, aplicações "agressivas" podem dominar a rede e o *provisioning* por si só não assegura prioridade na utilização da rede;
- Congestionamento pode surgir noutros pontos – Mesmo que uma parte da rede seja dimensionada, podem aparecer congestionamentos noutros segmentos da rede.

Um exemplo prático da utilização deste método, é uma empresa com 200 utilizadores verifica que, em horário de pico, o tráfego Internet atinge sensivelmente os 600 Mbps (videoconferência, *cloud* e *backups*). Para reduzir atrasos e perdas, decide garantir um acesso de 1 Gbps (*overprovisioning*) e atualizar a *firewall* e *uplinks* internos para 10 Gbps. Assim, mesmo com variações de utilização, a carga típica fica abaixo da capacidade, diminuindo a probabilidade de congestionamento.

5 – A frame Ethernet IEEE 802.3 é a unidade de dados da Camada 2 (*Data Link*) utilizada em redes Ethernet para transportar informação entre interfaces no mesmo domínio de broadcast. O formato 802.3 (estrito) distingue-se do Ethernet II porque o campo a seguir ao MAC de origem é *Length* (comprimento) e não *EtherType* (Tanenbaum, 2013). O formato da frame é o apresentado na seguinte imagem, seguindo-se uma descrição de cada campo.



Retirado de https://www.learncisco.net/courses/icnd-1/building-a-network/ethernet-protocol.html

1. *Preamble* (Preâmbulo) – Este campo marca o início da frame e tem um tamanho de 7 bytes, sendo formado pela repetição do padrão 10101010.

A sua função principal é permitir a sincronização entre emissor e recetor, isto é, ajudar o recetor a “alinhar” o seu relógio com o fluxo de bits antes de começar a interpretar os campos da frame. Em Ethernet clássica a 10 Mb/s (codificação Manchester), esta sequência produz transições regulares que facilitam a recuperação de relógio; no total, os 56 bits do preâmbulo ocupam 5,6 µs, preparando o recetor para a leitura do restante cabeçalho.

2. SFD ou SOF (*Start of Frame Delimiter*) – Tem 1 byte de tamanho e apresenta o padrão 10101011. É deliberadamente muito semelhante ao preâmbulo, mas termina com bits diferentes para marcar de forma inequívoca o fim da sincronização e o início efetivo da frame. Na prática, indica que o próximo campo a ser lido já é o endereço MAC de destino.
3. *Destination Address* (Endereço MAC de Destino) – O endereço de destino ocupa 6 bytes e identifica o dispositivo (ou grupo de dispositivos) para o qual a frame se dirige. Um aspeto importante é o primeiro bit que quando vale 0, o endereço é unicast (um único destinatário); quando vale 1, corresponde a multicast (um grupo). Um caso particular ocorre quando todos os bits do endereço estão a 1 (FF:FF:FF:FF:FF:FF), representando broadcast, ou seja, a frame deve ser entregue a todos os dispositivos no mesmo domínio de difusão.
4. *Source Address* (Endereço MAC de Origem) – O endereço de origem tem igualmente 6 bytes e indica o emissor da frame. Este identificador é, em geral, globalmente único, pois é atribuído com base em blocos reservados a fabricantes. Em particular, os primeiros 3 bytes correspondem ao OUI (Organizationally Unique Identifier), associado ao fabricante e atribuído pela IEEE, enquanto os restantes bytes completam a identificação específica do dispositivo.
5. *Length* (Comprimento) – No formato IEEE 802.3, este campo tem 2 bytes e representa o comprimento do conteúdo transportado (isto é, dos dados que seguem após este campo). Em Ethernet clássica, considera-se tipicamente o intervalo de 46 a 1500 bytes como carga útil efetiva, porque existe um tamanho mínimo e um tamanho máximo para a frame. Este valor não inclui preâmbulo, SFD, endereços MAC nem o campo de verificação (FCS/CRC). O limite superior de 1500 bytes está associado

ao MTU tradicional de Ethernet e a decisões de normalização/compatibilidade do padrão.

6. Data (Dados / *Payload*) – Este campo contém a carga útil (a informação que se pretende transportar, por exemplo um datagrama IP). O tamanho é variável: existe um mínimo (tipicamente 46 bytes) para garantir que a frame atinja o tamanho mínimo exigido pela Ethernet clássica; caso o conteúdo real seja menor, são acrescentados bytes de enchimento (padding). Este requisito está historicamente ligado à necessidade de deteção de colisões em redes half-duplex com CSMA/CD, garantindo que uma transmissão dura tempo suficiente para a colisão ser detetável. O limite máximo (1500 bytes) resulta de escolhas de engenharia e das restrições tecnológicas e de interoperabilidade definidas na especificação.
7. FCS (*Frame Check Sequence*) – Este é o último campo, com 4 bytes, calculado através de um CRC-32. O emissor calcula este valor a partir do conteúdo da frame (do endereço de destino até ao fim dos dados/padding) e o recetor recalcula-o para comparação. Se os valores não coincidirem, conclui-se que houve erro na transmissão e a frame é rejeitada (descartada).

6.a – O algoritmo de roteamento Inundação (flooding) é uma técnica muito simples em que um nó (router) ao receber um pacote não escolhe um único próximo salto, em vez disso, reencaminha o pacote por todas as interfaces de saída, exceto pela interface por onde o pacote entrou (Tanenbaum, 2013). O funcionamento do algoritmo é o seguinte (Tanenbaum, 2013):

1. **Transmissão inicial –** Quando um router recebe um pacote, procede ao seu reencaminhamento por todas as interfaces de saída, com exceção da interface pela qual o pacote entrou. Deste modo, a informação propaga-se pela rede e tende a alcançar todos os nós alcançáveis.
2. **Replicação do tráfego –** Como o pacote é enviado simultaneamente por múltiplos enlaces, são geradas várias cópias que se espalham por caminhos diferentes. Esta multiplicação aumenta

significativamente o volume de tráfego e pode originar congestionamento e receção de cópias redundantes.

3. **Mecanismos de controlo –** Para limitar loops e reduzir sobrecarga, utilizam-se mecanismos como:
    a. TTL (Time-to-Live) / contador de saltos – Cada pacote transporta um valor de TTL que é decrementado em cada router; quando o valor chega a zero, o pacote é descartado, evitando propagação indefinida.
    b. Eliminação de duplicados – Cada pacote inclui um identificador único (por exemplo, origem + número de sequência). Os routers mantêm um registo dos identificadores já observados e, ao receberem um duplicado, não o reenviam.
4. **Chegada ao destino –** Quando pelo menos uma das cópias atinge o nó de destino, considera-se que a entrega foi bem-sucedida; as cópias remanescentes acabam por expirar (via TTL) ou ser descartadas por deteção de duplicação.

No esquema apresentado na questão, o flooding funcionaria assim (assumindo controlo por "não reenviar para o enlace de entrada"):

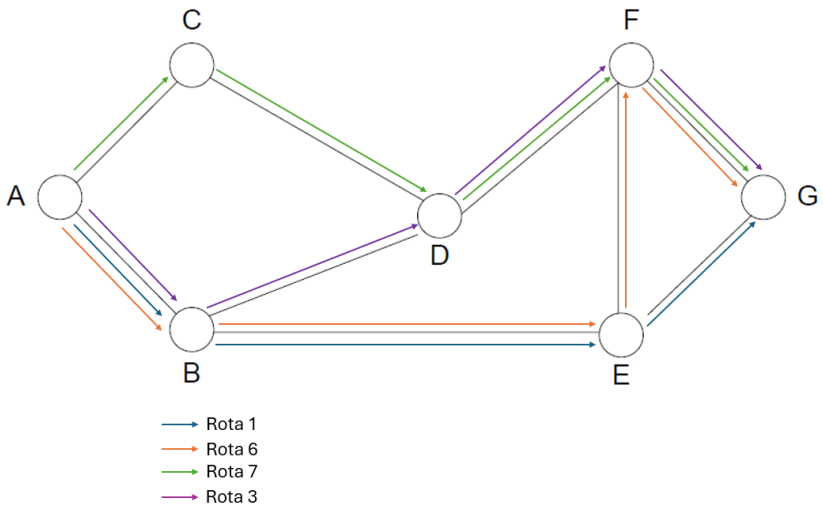
- **A** envia para **B** e **C**.
- **B** reenvia para **D** e **E** (exceto **A**) e **C** reenvia para **D** (exceto **A**).
- **D** recebe cópias (de **B** e **C**) processando a primeira e descarta duplicados, depois reenvia por todas as saídas exceto a de entrada, isto é, para **F** e para o outro nó (**B** ou **C**).
- **E** ao receber reenvia para todas as saídas exceto a de entrada, tipicamente **F** e **G** se recebeu de **B**, ou **B** e **G** se recebeu de **F**.
- **F** ao receber reenvia para todas as saídas exceto a de entrada, por exemplo **E** e **G** se recebeu de **D**, ou **D** e **G** se recebeu de **E**.
- **G** pode receber por **E** e por **F**, aceitando a primeira cópia e descartando as restantes como duplicadas.

Sem controlo, haveria loops no triângulo E–F–G e também no ciclo B–D–F–E–B, gerando tráfego repetido, com TTL e ID de pacotes, a inundação termina quando o TTL expira e os duplicados deixam de ser reenviados.

6.b – Utilizando o algoritmo de flooding, numa transmissão iniciada em A com destino a G, assumindo que cada nó não reencaminha pela ligação de entrada, que descarta pacotes duplicados (com base num identificador) e que existe um limite máximo de 4 hops (TTL=4), obtêm-se os seguintes percursos possíveis:

- Rota 1: A → B → E → G — a cópia chega ao destino em 3 hops.
- Rota 2: A → B → D → C → A — a cópia não chega a G e é descartada em A por ser duplicada.
- Rota 3: A → B → D → F → G — a cópia chega ao destino em 4 hops.
- Rota 4: A → B → D → F → E — o TTL expira em E (4.º hop), pelo que a cópia é descartada e não chega a G.
- Rota 5: A → B → E → F → D — o TTL expira em D (4.º hop), pelo que a cópia é descartada e não chega a G.
- Rota 6: A → B → E → F → G — a cópia chega ao destino em 4 hops.
- Rota 7: A → C → D → F → G — a cópia chega ao destino em 4 hops.
- Rota 8: A → C → D → B → A — a cópia não chega a G e é descartada em A por ser duplicada.
- Rota 9: A → C → D → B → E — o TTL expira em E (4.º hop), pelo que a cópia é descartada e não chega a G.
- Rota 10: A → C → D → F → E — o TTL expira em E (4.º hop), pelo que a cópia é descartada e não chega a G.

Assim, com TTL=4, apenas as rotas 1, 3, 6 e 7 conseguem entregar uma cópia em G; as restantes terminam por duplicação (rotas 2 e 8) ou por expiração do TTL (rotas 4, 5, 9 e 10).



6.c – Assumindo o flooding controlado definido, ou seja, não reencaminhar pela ligação de entrada, rejeitar duplicados e o TTL = 4 hops, o custo em largura de banda não é apenas o caminho até G, mas sim a soma de todas as transmissões (cópias) efetuadas em cada ligação até o TTL expirar / os duplicados serem descartados.

Considerou-se que:

- Cada reencaminhamento numa ligação consome 1 “hop de largura de banda” (uma transmissão do pacote nessa ligação);
- Um pacote enviado de A para B e C chega mais rápido a C do que a retransmissão através da rota A → B → D → C, e vice-versa, e para as demais hipóteses similares;
- Um pacote é recebido e enviado antes da receção de outro pacote por uma ligação diferente.

Assim, a contagem de transmissões (hops) na rede, é a seguinte:

- A envia para B e C → 2 hops
- B reenvia para D e E, e C reenvia para D → 3 hops
- D (processa a 1.ª cópia e ignora a duplicada) reenvia para F e para o outro vizinho (B ou C) e E reenvia para F e G → 4 hops
- F (processa a 1.ª cópia e ignora duplicadas) reenvia para G e para (D ou E) → 2 hops (Os nós que recebem aqui ficam com TTL=0 e não reenviam.)

Total de hops (transmissões) consumidos na rede: 2+3+4+2=11 $hops$

Embora o destino G possa ser alcançado em 3 hops (A→B→E→G), no flooding o pacote é replicado e atravessa vários enlaces em paralelo; por isso, o consumo de largura de banda é proporcional ao número total de transmissões: 11 × (tamanho do pacote).

7.a – O *Distance-Vector Routing* (DVR) é uma abordagem de roteamento dinâmico, distribuída e iterativa, na qual cada router mantém uma tabela de roteamento indexada por todos os destinos conhecidos na rede. Para cada destino, essa tabela contém, pelo menos, duas informações essenciais: uma estimativa do custo total para alcançar o destino e a indicação do próximo salto, isto é, a interface de saída ou router vizinho a utilizar para seguir o

caminho considerado ótimo. O conceito de “melhor” caminho é tipicamente definido como o de menor custo, podendo a métrica de custo corresponder ao número de saltos (hops) ou a outras grandezas relevantes para a rede, como atraso, largura de banda ou fiabilidade. Dependendo do protocolo, alguns custos podem ser configurados administrativamente ou estimados através de medições associadas à ligação entre vizinhos (Tanenbaum, 2013).

O funcionamento do DVR baseia-se na troca periódica de informação apenas entre vizinhos diretos, não exigindo que cada router possua uma visão global da topologia. Em intervalos regulares, e também quando ocorre uma alteração significativa, cada router anuncia aos seus vizinhos o seu “vetor de distâncias”, ou seja, as melhores estimativas que possui para atingir cada destino. Quando um router recebe o vetor de distâncias de um vizinho, procede à atualização da sua própria tabela aplicando o princípio do algoritmo de Bellman–Ford: para cada destino, compara o custo atualmente registado com o custo de chegar ao mesmo destino passando pelo vizinho emissor, calculado como a soma do custo do enlace até esse vizinho com o custo anunciado pelo vizinho para o destino em causa. Se esta soma produzir um valor inferior ao anteriormente conhecido, a tabela é atualizada e o próximo salto passa a ser o vizinho que originou a melhoria. Caso uma atualização altere a tabela, essa alteração pode desencadear novos anúncios, propagando gradualmente a informação pela rede até que as tabelas deixem de se modificar, atingindo-se assim a convergência, isto é, um estado em que todos os routers refletem de forma consistente os melhores caminhos para os destinos, de acordo com a topologia e os custos vigentes (Tanenbaum, 2013).

Apesar da simplicidade e do baixo custo de operação, o DVR apresenta limitações reconhecidas. Em particular, tende a convergir de forma mais rápida quando surgem rotas melhores, mas pode convergir lentamente perante falhas ou remoções de routers e ligações, devido ao fenómeno conhecido como *count-to-infinity*, no qual anúncios desatualizados podem manter rotas incorretas temporariamente e, em certos casos, induzir ciclos de roteamento até a informação correta se propagar por toda a rede. Por este motivo, protocolos baseados em vetor de distância recorrem frequentemente a mecanismos complementares para reduzir o impacto destas situações, como

split horizon, *poison reverse*, temporizadores de *hold-down* e atualizações desencadeadas. O DVR é, por isso, frequentemente descrito como a aplicação distribuída do algoritmo de Bellman–Ford ao roteamento e encontra expressão em protocolos históricos e amplamente conhecidos, como o RIP (*Routing Information Protocol*), que utiliza uma métrica simples baseada no número de hops (Tanenbaum, 2013).

7.b – Apresenta-se a rede com os custos associados, de acordo com os valores fornecidos, organizados numa tabela de apoio, tendo-se deduzido que os valores dados, seguem a ordem: A, B, C, D, E, F; pois cada vetor tem 0 na posição do próprio router.

		Origem		
		B	**D**	**E**
Destino	**A**	5	16	7
	B	0	12	6
	C	8	6	3
	D	12	0	9
	E	6	9	0
	F	2	10	4

Para atualizar a tabela de encaminhamento do router C, são conhecidos os novos retardos medidos nas ligações diretas para os seus vizinhos imediatos: C→B = 6, C→D = 3 e C→E = 5. Resta, portanto, determinar o menor custo estimado para alcançar os routers que não pertencem à vizinhança direta de C, nomeadamente A e F, com base nos vetores anunciados pelos vizinhos B, D e E.

Para obter o custo total estimado de C até um destino não adjacente, procede-se do seguinte modo: para cada vizinho candidato (B, D e E), soma-se o custo do enlace direto C→vizinho ao custo anunciado por esse vizinho para o destino. Em seguida, seleciona-se o menor dos valores obtidos, que define simultaneamente o retardo esperado e o próximo hop (linha de saída) a utilizar.

No caso do destino A, existem três possibilidades via os vizinhos de C: via B, via E e via D. Assim, calculam-se os seguintes custos totais:

- Via **B**: $CB + BA = 6 + 5 = 11$
- Via **E**: $CE + EA = 5 + 7 = 12$
- Via **D**: $CD + DA = 3 + 16 = 19$

- Conclui-se que o menor custo para C alcançar A é via B, com retardo 11.

Aplicando o mesmo procedimento ao destino F, novamente com as três alternativas (via B, via E e via D), obtêm-se:

- Via **B**: $CB + BF = 6 + 2 = 8$
- Via **E**: $CE + EF = 5 + 4 = 9$
- Via **D**: $CD + DF = 3 + 10 = 13$
- Deste modo, o menor custo para C alcançar F é também via B, com retardo 8.

Por fim, apresenta-se a tabela global atualizada, onde se registam, para cada destino, o próximo hop escolhido e o retardo total esperado a partir de C.

Destino	Saída	Retardo
A	B	11
B	B	6
C	-	0
D	D	3
E	E	5
F	B	8

Bibliografia:

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2013). *Computer Networks* (6th ed.; Pearson New International Edition). Pearson.