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

SISTEMAS EM REDE | 21106

A preencher pelo estudante

UNIDADE CURRICULAR: Sistemas em Rede

CÓDIGO: 21106

DOCENTE: Arnaldo Santos e Henrique São Mamede

NOME: Yrma Marina Vianez Martins

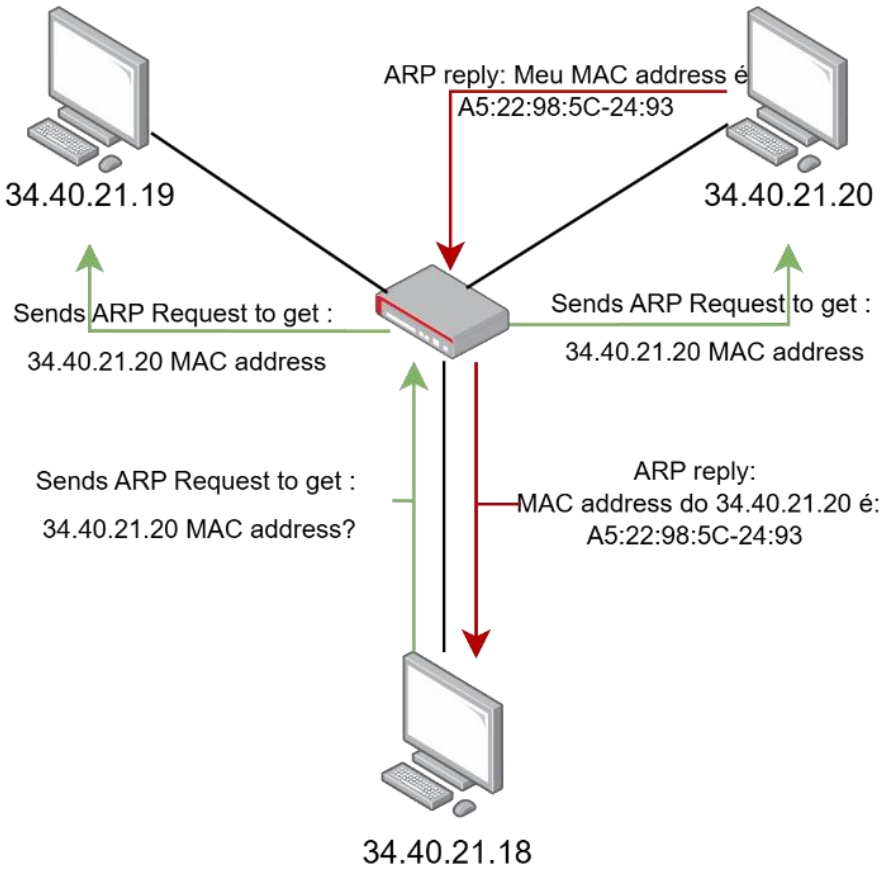
N.º DE ESTUDANTE: 2300212

CURSO: Engenharia Informática

TRABALHO / RESOLUÇÃO:

1.O **ARP (Address Resolution Protocol)** é um protocolo fundamental para o funcionamento de redes locais, projetado para traduzir endereços IP (lógicos, de 32 bits) em endereços MAC (físicos, de 48 bits) e vice-versa. Introduzido na RFC 826 em 1982, o ARP é crucial para a comunicação em redes baseadas em IPv4, como Ethernet, permitindo que dispositivos na mesma rede local troquem informações de forma eficiente. Este protocolo funciona na intersecção das camadas 2 (Data Link) e 3 (Network) do modelo OSI, já que os endereços IP pertencem à camada Network e os endereços MAC à camada de Data Link.

O ARP funciona por meio de mensagens de solicitação e resposta. Quando um dispositivo deseja comunicar-se com outro na rede local e conhece apenas o endereço IP do destinatário, ele verifica a sua tabela de cache ARP para encontrar o endereço MAC correspondente. Se não encontrar essa informação, envia uma mensagem **ARP Request** em broadcast, a perguntar: "Quem tem o endereço IP X?" O dispositivo que possui o IP requisitado responde diretamente ao emissor com uma mensagem **ARP Reply**, indicando o seu endereço MAC. Ambas as máquinas, então armazenam a associação IP-MAC nas suas tabelas ARP, otimizando futuras comunicações.



Além do funcionamento básico, o ARP apresenta várias variantes que ampliam a sua utilidade em diferentes cenários. O **Proxy ARP**, por exemplo, permite que um dispositivo responda a solicitações ARP em nome de outro, facilitando a comunicação entre sub-redes. O **Gratuitous ARP** é usado para anunciar um endereço IP e seu respetivo MAC sem solicitação prévia, sendo útil para detetar conflitos de IP ou atualizar tabelas ARP de outros dispositivos na rede. Já o **Inverse ARP (INARP)** realiza a operação inversa, resolvendo endereços MAC para IP, e é frequentemente utilizado em redes como Frame Relay. Por outro lado, o **ARP Spoofing** ou envenenamento de cache (DNS cache poisoning) que é uma técnica maliciosa que explora vulnerabilidades do protocolo, permitindo que atacantes redirecionem tráfego ou realizem man-in-the-middle (MITM).

O ARP é uma ferramenta poderosa, mas tem limitações. Ele não é compatível com redes IPv6, que utilizam o NDP (Neighbor Discovery Protocol) para desempenhar funções similares. Além disso, a sua vulnerabilidade a ataques de destaca a necessidade de implementar contramedidas, como listas de acesso ou switches com funcionalidades de segurança avançadas.

2. O formato de uma Frame Ethernet, de acordo com o padrão 802.3, é composto por diversos campos com funções e tamanhos específicos, garantindo uma comunicação eficiente e fiável em redes locais. A estrutura da frame é a seguinte:

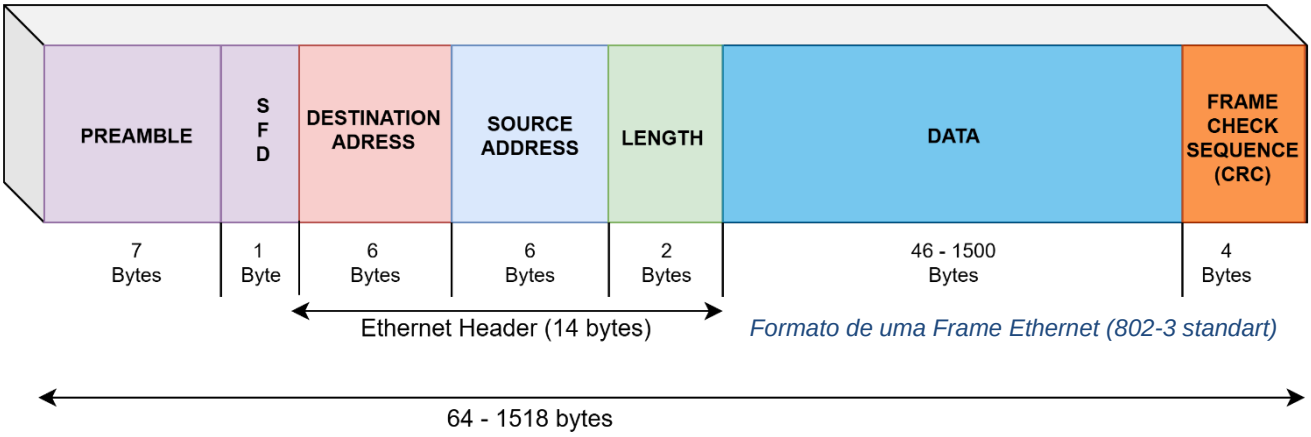
1. Preamble (Preâmbulo): Este campo tem um tamanho de 7 bytes e é constituído pelo padrão de bits 10101010. A sua função é sincronizar o clock do transmissor com o do recetor, permitindo que o dispositivo recetor esteja preparado para processar os dados que vão ser transmitidos. A codificação Manchester deste padrão gera uma onda quadrada de 10 MHz durante 6,4 µs, facilitando a sincronização.
2. Start of Frame Delimiter (SFD): Este campo, com 1 byte, contém o padrão 10101011, semelhante ao preamble mas com os dois últimos bits diferentes. A sua função é indicar o início da frame Ethernet, sinalizando que os bits seguintes correspondem ao endereço de destino. Em algumas referências, o SFD é considerado parte do preamble, levando à designação de 8 bytes para este último.

3. Destination Address (Endereço de Destino): Este campo é composto por 6 bytes e contém o endereço MAC do dispositivo ao qual os dados são destinados. O primeiro bit deste endereço determina o tipo de destino: 0 para unicast (endereço

individual) e 1 para multicast (endereços de grupo). Quando todos os bits estão a 1, o endereço é de broadcast, indicando que a frame deve ser enviada a todos os dispositivos na rede.

4. Source Address (Endereço de Origem): Também com 6 bytes, este campo contém o endereço MAC do dispositivo emissor. Este endereço é globalmente único e atribuído pelo IEEE (Institute of Electrical and Electronics Engineers), garantindo que não existam endereços duplicados. Os primeiros 3 bytes deste campo correspondem ao OUI (Organizationally Unique Identifier), identificador exclusivo do fabricante do dispositivo.
5. Length (Comprimento): Com um tamanho de 2 bytes, este campo especifica o tamanho dos dados contidos na frame, variando entre 46 e 1500 bytes. Este campo exclui os bytes referentes ao preâmbulo, SFD, endereços de destino, origem, e CRC. O limite de 1500 bytes é uma limitação técnica do padrão Ethernet.
6. Data (Dados): Este é o campo que contém a carga útil da frame, ou seja, os dados que estão a ser transmitidos. O tamanho deste campo pode variar entre 46 e 1500 bytes. O tamanho mínimo é necessário para evitar colisões na rede, enquanto o tamanho máximo foi definido com base nas limitações tecnológicas da época em que o padrão Ethernet foi criado (1978), nomeadamente os custos elevados da memória RAM.
7. CRC (Cyclic Redundancy Check): Este campo de 4 bytes é utilizado para verificar a integridade dos dados transmitidos. O CRC calcula um valor com base no conteúdo da frame, e este valor é comparado pelo recetor com um cálculo próprio. Se houver discrepâncias, a frame é descartada.

Esta estrutura da Frame Ethernet foi desenvolvida com o objetivo de garantir eficiência e fiabilidade nas comunicações. O preamble e o SFD asseguram uma sincronização adequada, enquanto os campos de endereço garantem o envio e receção para o dispositivo correto. Por fim, o CRC valida a integridade dos dados, assegurando que não houve corrupção durante a transmissão. Este design tornou o padrão Ethernet num dos mais utilizados em redes locais.



Formato de uma Frame Ethernet (802-3 standart)

3. Uma LAN (Local Area Network) é uma rede privada projetada para operar dentro de uma área geográfica limitada, como um edifício, escritório ou campus. Permite a interligação de dispositivos, como computadores, impressoras e outros, para a partilha de recursos e troca de informações. Existem dois tipos principais de LAN: as com fios, que utilizam cabos de cobre ou fibra ótica, oferecendo maior velocidade e fiabilidade, e as sem fios (Wi-Fi), que operam com rádio modems e antenas para comunicar com pontos de acesso, facilitando a mobilidade e a instalação em locais onde a cablagem é inviável. As LANs com fios geralmente utilizam a tecnologia Ethernet (IEEE 802.3), onde os dispositivos se conectam a switches através de enlaces ponto-a-ponto. Numa LAN, podem estar presentes vários elementos, como switches e hubs, que interligam fisicamente os dispositivos, roteadores, que conectam a LAN a outras redes como a Internet, e computadores, sejam desktops ou portáteis, que são os dispositivos principais utilizados para trabalho e comunicação. Além disso, podem incluir impressoras, scanners e servidores, que armazenam ficheiros, gerem bases de dados e fornecem serviços aos utilizadores na rede, bem como câmaras de segurança IP para monitorização, telefones VoIP para comunicação, sistemas de armazenamento como NAS ou SAN para gestão de dados centralizados, dispositivos IoT, como sensores e controladores, e pontos de acesso (APs) para estender a conectividade sem fios. Para assegurar o desempenho e a segurança da rede, é comum incluir firewalls e sistemas de gestão de rede. Desta forma, uma LAN é estruturada para otimizar a conectividade, partilha de recursos e a proteção de dados.

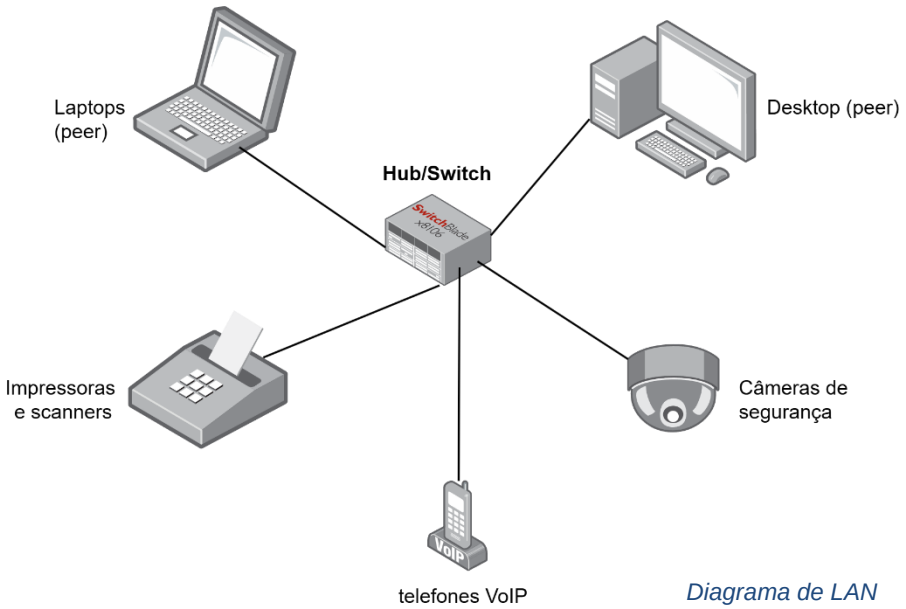


Diagrama de LAN

Uma WAN (Wide Area Network), por outro lado, cobre uma vasta área geográfica, como países ou continentes, permitindo a interligação de várias LANs. Estas redes utilizam infraestruturas compostas por linhas de transmissão, como fios de cobre, cabos coaxiais, fibra ótica ou comunicações via satélite, e dispositivos de comutação, como routers, que encaminham os dados entre diferentes redes. São amplamente utilizadas para conectar escritórios localizados em diferentes regiões, frequentemente através da Internet, utilizando VPNs ou provedores de serviços de rede.

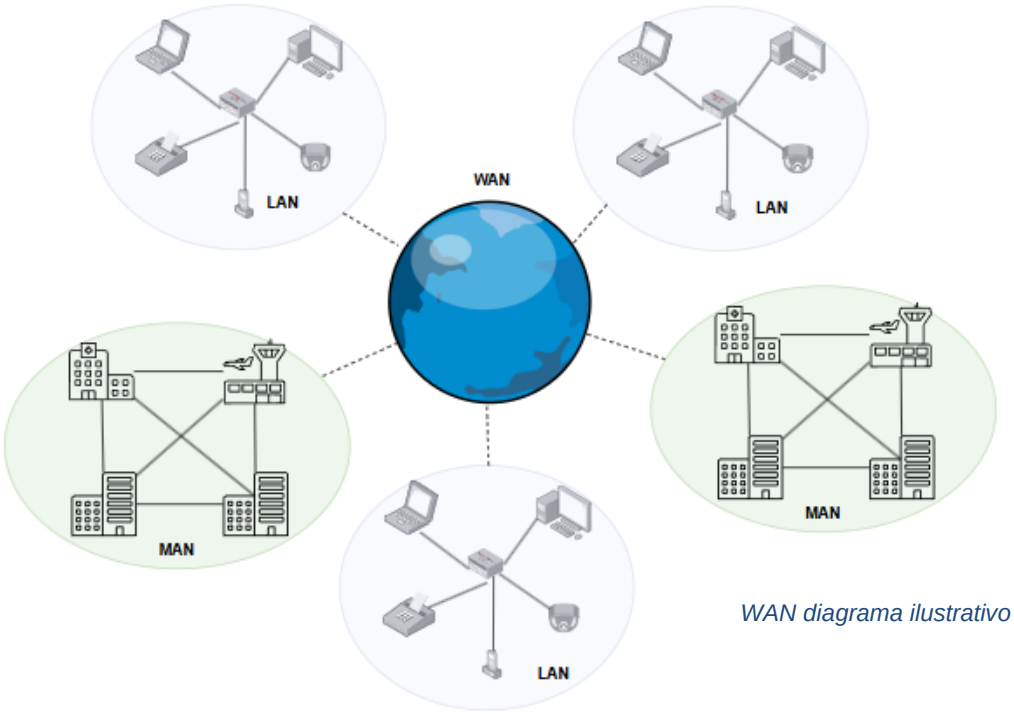
As WANs distinguem-se por apresentarem uma separação clara entre as sub-redes e os hosts que as compõem. Estas redes podem ser configuradas de diversas formas, como por meio de VPNs, que proporcionam maior flexibilidade e aproveitamento de recursos existentes, ou através de sub-redes operadas por provedores de serviços de rede, como os ISPs (Internet Service Providers), que conectam vários clientes e os integram à Internet.

As WANs podem incluir redes MAN (Metropolitan Area Networks), que cobrem áreas geográficas menores, como cidades ou regiões metropolitanas, interligando múltiplas LANs dentro de uma mesma área através de infraestruturas de alta velocidade, como fibra ótica. As MANs servem como um intermediário entre as LANs locais e a WAN, otimizando a conectividade em áreas urbanas.

As WANs modernas também incluem tecnologias sem fios, como redes via satélite, que possibilitam a cobertura de áreas remotas e de grande extensão geográfica, sendo a iniciativa Starlink um exemplo relevante desse tipo de tecnologia.

No contexto de LANs, existem vantagens e desvantagens ao comparar uma LAN sem fios (Wi-Fi) com uma LAN com fios (fibra ou cobre). As LANs sem fios oferecem vantagens significativas, como maior mobilidade, uma vez que os dispositivos podem conectar-se à rede em qualquer local dentro da área de cobertura, e facilidade de instalação, já que não é necessário instalar cablagem física, tornando-a mais prática e menos dispendiosa em locais onde a infraestrutura de fios é inviável. No entanto, também apresentam desvantagens, como velocidades e fiabilidade inferiores devido à suscetibilidade a interferências, como paredes ou outros dispositivos eletrónicos, e menor segurança, pois são mais vulneráveis a acessos não autorizados ou interceções de dados, exigindo configurações de segurança adicionais. Por outro lado, as LANs com fios possuem vantagens como velocidades mais elevadas e estáveis, alcançando até 10 Gbps com Ethernet moderna, além de maior segurança devido à natureza confinada das conexões físicas, dificultando acessos não autorizados.

Contudo, apresentam desvantagens como a restrição de mobilidade, já que os dispositivos precisam de estar fisicamente conectados, e custos de instalação mais elevados, devido à necessidade de cabos e à complexidade de instalação em certos locais.



WAN diagrama ilustrativo

4.a) Flooding é um algoritmo simples e robusto usado para encaminhar pacotes numa rede. Neste algoritmo, cada router que recebe um pacote reencaminha-o por todas as suas ligações disponíveis, com exceção da ligação por onde o pacote foi recebido, garantindo assim que o pacote alcance todos os destinos possíveis na rede.

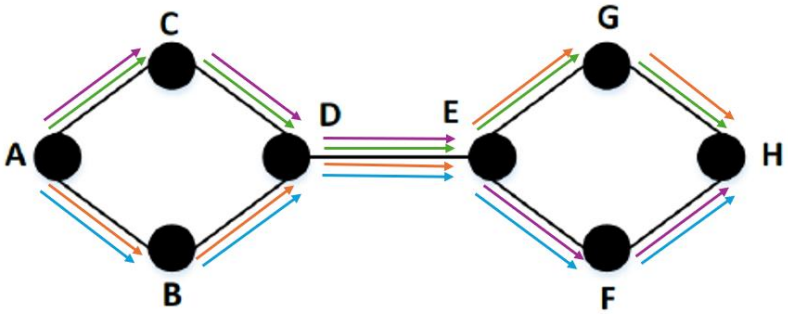
O funcionamento baseia-se no envio indiscriminado de pacotes. Este processo é repetido por todos os routers da rede, fazendo com que o pacote se propague por todos os caminhos possíveis. Para evitar que o pacote circule indefinidamente, utilizam-se mecanismos de controlo, como o TTL (Time to Live). O TTL é um contador que diminui a cada hop e, ao atingir zero, faz com que o pacote seja descartado. Outra abordagem usada é manter uma lista de pacotes já recebidos em cada router, permitindo identificar e descartar pacotes duplicados.

O algoritmo de Flooding apresenta algumas vantagens, como a alta fiabilidade, já que o pacote é enviado por todas as rotas possíveis, garantindo a entrega mesmo em caso de falha em alguns caminhos. Além disso, é relativamente simples de implementar. Contudo, também tem desvantagens, como a ineficiência no uso de largura de banda,

pois os pacotes são enviados múltiplas vezes, mesmo por rotas desnecessárias, gerando redundância e sobrecarregando a rede.

No exemplo apresentado no grafo, um pacote que tem origem no router A, este inicia o envio do pacote e transmite-o para os routers B e C. O router B, ao receber o pacote de A, reencaminha-o apenas para D, uma vez que não reenvia para A. De forma semelhante, o router C, ao receber o pacote de A, reencaminha-o também para D. Quando o router D recebe o pacote, este pode vir de B ou C. Independentemente disso, D reencaminha o pacote para E, mas não volta a enviá-lo para B nem para C, pois são os routers por onde o pacote já chegou. O router E, ao receber o pacote de D, reencaminha-o para os routers F e G, e eventualmente para D, mas neste último caso, o pacote será descartado por duplicação no destino. Por sua vez, o router F, ao receber o pacote de E, reencaminha-o para H, mas não volta a enviá-lo para E. O mesmo acontece com o router G, que, ao receber o pacote de E, reencaminha-o também para H, mas não devolve para E. Finalmente, o router H, ao receber o pacote de F e G, não reencaminha o pacote para mais ninguém, pois todas as possíveis rotas já foram percorridas. Com o algoritmo de Flooding, todos os routers da rede (de A a H) acabam por receber o pacote, garantindo que ele chegue ao destino, independentemente do caminho seguido. Contudo, devido à redundância gerada e à sobrecarga na rede, este algoritmo é mais adequado para situações específicas e é geralmente substituído por algoritmos mais eficientes em cenários reais.

4.b) Se um pacote é enviado de A para H com uma contagem máxima de hops = 5, o algoritmo de Flooding garante que o pacote será enviado por todas as rotas possíveis, respeitando o limite de 5 hops para cada percurso. De acordo com o grafo e as setas coloridas que acrescentei para identificar as possíveis rotas que o pacote seguirá:



Rotas possíveis:	tamanho
A→C→D→E→F→H	5 hops
A→C→D→E→G→H	5hops
A→B→D→E→G→H	5 hops
A→B→D→E→F→H	5 hops

Todas as rotas foram identificadas considerando a retransmissão do pacote em cada router (exceto para o router de origem), sem ultrapassar o limite máximo de 5 hops. Este limite garante que o pacote seja descartado automaticamente se exceder o número de transmissões permitido.

Para calcular o consumo de largura de banda, é necessário contabilizar todas as transmissões realizadas no grafo. No algoritmo de Flooding, cada ligação entre routers é utilizada uma vez em cada rota possível dentro do limite de hops permitido. Contudo, o algoritmo também elimina pacotes duplicados assim que eles chegam a routers já percorridos, o que reduz o número total de transmissões efetivas.

O cálculo do consumo de largura de banda baseia-se nas transmissões realizadas pelo pacote enquanto percorre as diversas rotas possíveis no grafo. Primeiro, o pacote é enviado do router A para os routers C e B, resultando em 2 transmissões iniciais (uma para cada ligação). Depois, o pacote segue de C para D e de B para D, somando mais 2 transmissões, já que cada router reencaminha o pacote para o próximo.

Independentemente do caminho inicial, o pacote que chega ao router D é enviado para o router E, representando 1 transmissão adicional, pois todos os pacotes passam por essa ligação. A partir de E, o pacote é transmitido simultaneamente para os routers F e G, adicionando mais 2 transmissões. Finalmente, os pacotes transmitidos de E para F e G seguem até o destino H, completando o percurso com 2 transmissões finais (uma de F → H e outra de G → H).

Resumindo numa tabela, temos:

A → C	1 transmissão
A → B	1 transmissão
C → D	1 transmissão
B → D	1 transmissão
D → E	1 transmissão
E → F	1 transmissão
E → G	1 transmissão
F → H	1 transmissão
G → H	1 transmissão
Total	9 transmissões

O algoritmo de Flooding garante que o pacote atinja o destino H utilizando 9 hops únicos, correspondendo a 9 transmissões efetivas no grafo. Embora múltiplas rotas tenham sido exploradas, os pacotes duplicados foram eliminados em cada router, de modo que apenas as transmissões necessárias foram contabilizadas.

A contagem de 9 hops reflete o número total de ligações percorridas no grafo e, consequentemente, o consumo de largura de banda neste cenário.

5.a) O algoritmo DVR (Distance Vector Routing), também conhecido como roteamento por vetor de distância, é um método que funciona através da troca de informações entre routers de uma rede para determinar o melhor caminho até cada destino. Cada router mantém uma tabela que indica a distância conhecida até todos os destinos na rede e o próximo hop necessário para alcançá-los. Inicialmente, cada router possui uma tabela de routing que lista todos os destinos possíveis, atribuindo distâncias iniciais. Para os vizinhos diretos, a distância é conhecida, enquanto para os outros destinos a distância é definida como infinita. Periodicamente, cada router envia a sua tabela de routing para os seus vizinhos, incluindo as distâncias para todos os destinos que conhece.

Quando um router recebe uma tabela de routing de um vizinho, ele recalcula a distância para cada destino com base nas informações recebidas. O custo para alcançar um destino é calculado somando a distância até o vizinho e a distância do vizinho até o destino. Caso a nova rota seja mais curta do que a que já estava registada, o router atualiza a sua tabela para refletir a nova rota. Este processo de troca de tabelas e atualização continua até que todos os routers na rede possuam uma visão consistente e otimizada das distâncias, alcançando assim a convergência.

Embora o algoritmo seja simples e eficiente em redes pequenas ou médias, ele apresenta algumas limitações. Uma delas é a lentidão na convergência em redes grandes ou em situações de falha. Além disso, o algoritmo pode sofrer do problema de "contagem ao infinito", em que routers entram num ciclo ao aumentar indefinidamente a distância para um destino inacessível. Apesar dessas desvantagens, o algoritmo é amplamente utilizado e é a base de protocolos de routing como o RIP (Routing Information Protocol), sendo reconhecido pela sua simplicidade e capacidade de se adaptar dinamicamente às mudanças na topologia da rede.

5.b) No enunciado, são fornecidos os vetores de distância recebidos pelo Router C, assim como os retardos medidos para os routers B, D e E, que são:

- de B (retardo 6): (5, 0, 8, 12, 6, 2)
- de D (retardo 3): (16, 12, 6, 0, 9, 10)
- de E (retardo 5): (7, 6, 3, 9, 0, 4)

Com isto, calculo então o retardo esperado, que é simplesmente somar o vetor com o retardo de cada router. Para cada destino, o custo total foi obtido adicionando o valor do vetor (custo informado pelo vizinho) ao retardo associado ao respetivo router. Por exemplo, para alcançar o destino A via B, o custo foi calculado como 5 (vetor de B) + 6

(retardo de B) = 11. Este processo foi repetido para todos os destinos, considerando as três possibilidades (via B, D e E).

Na Tabela 1, os menores custos para cada destino estão destacados a verde, indicando os caminhos mais eficientes. Por exemplo, para o destino A, o menor custo é 11, destacado a verde, que corresponde ao caminho via B. O mesmo acontece para os restantes destinos: o menor custo indica o next hop a ser utilizado para alcançar cada destino da forma mais eficiente. Estes valores destacados são usados para construir a tabela de roteamento final do router C, apresentada na Tabela 2, garantindo o menor retardo esperado para cada destino na rede.

Como já identifiquei os menores custos, é possível determinar o next hop e o custo total para cada destino. O next hop corresponde ao router vizinho (B, D ou E) que oferece o menor custo total para alcançar o destino, garantindo assim o caminho mais eficiente na rede. Com base nesses menores custos, a tabela de roteamento final foi construída (Tabela 2). Por fim, o vetor transmitido pelo Router C é: (11, 6, -, 3, 5, 8), onde o "-" indica que o router C é o próprio destino e, portanto, não necessita de next hop.

Router	Vetores B	Vetores soma retardo B	Vetores D	Vetores soma retardo D	Vetores E	Vetores soma retardo E
A	5	5+6=11	16	16 + 3 = 19	7	7+5=12
B	0	0+6 =6	12	12 + 3 = 15	6	6 + 5 = 11
C	8	8+6 =14	6	6 + 3 = 9	3	3 + 5 = 8
D	12	12+6 = 18	0	0 + 3 = 3	9	9 + 5 = 14
E	6	6+6 =12	9	9 + 3 = 12	0	0 + 5 = 5
F	2	2+6=8	10	10 + 3 = 13	4	4 + 5 = 9

Tabela 1

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

Tabela 2

Bibliografia:

Apresentações de apoio fornecidas pelo professor no fórum

Tanenbaum, Feamster, Wetherall, Computer Networks. 6th Edition,

https://wiki.dcet.uab.pt/files/index.php/Categoria:Engenharia_Inform%C3%A1tica

https://chatgpt.com/

https://www.techtarget.com/searchnetworking/definition/Address-Resolution-Protocol-ARP

https://www.youtube.com/watch?v=45mEezqpvNw