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

NOME: Júlio César Gomes de Barros

N.º DE ESTUDANTE: 1902295

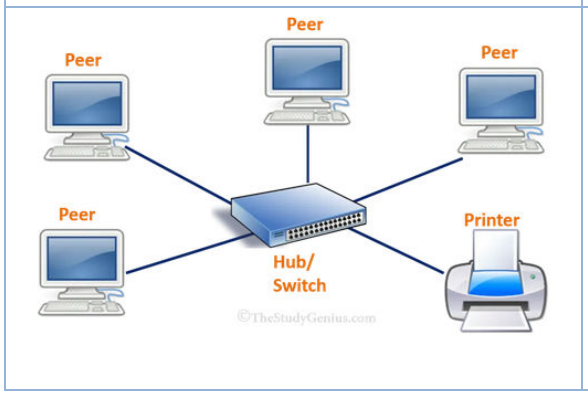
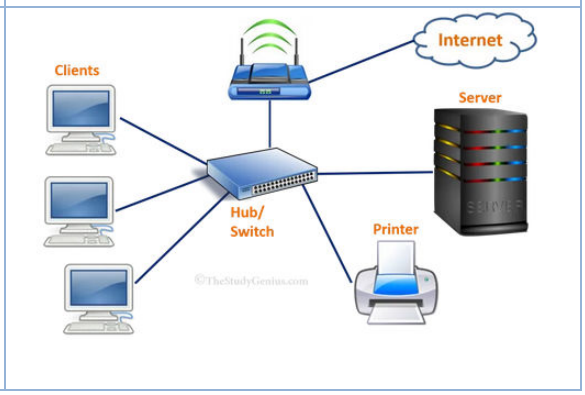
CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 04/01/2023

1) **LAN** (Local Area Network) ou Rede de Área Local e **WAN** (Wide Area Network) Rede de Área Alargada, ou de grande extensão, atendendo à designação, distinguem-se imediatamente pela dimensão física ou geográfica que o nome pretende evidenciar.

De menor dimensão a PAN (Personal Area Network), que pode ser constituída apenas por uma ligação simples como a que se estabelece por Bluetooth entre um smartwatch e um telemóvel, ou algum dos múltiplos equipamentos IoT (Internet Of Things) que atualmente proliferam, dotando por exemplo uma simples lâmpada de capacidade de comunicação.

Uma rede de área local, LAN, é uma rede de dimensão relativamente reduzida, que pode ir de um sistema caseiro com um router wifi, um telemóvel e uma SmartTV, até milhares de computadores distribuídos por alguns edifícios próximos ligados entre si, podendo uma LAN ser do tipo ponto-a-ponto (P2P) onde qualquer dos dispositivos pode atuar como cliente e/ou servidor, como acontece normalmente em redes LAN domésticas, ou do tipo cliente-servidor, típicas de ambientes que carecem de redes bem estruturadas, como empresas, industria, escolas, etc, com inúmeros clientes/terminais e alguns servidores, por exemplo para aplicações, ficheiros, correio eletrónico, etc.

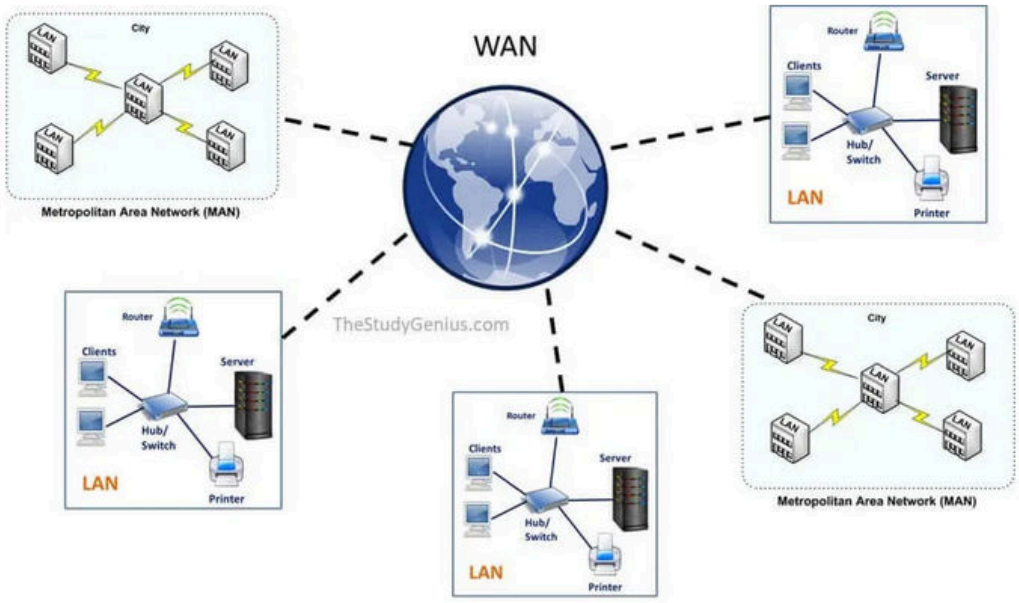
[1] LAN tipo P2P	LAN tipo cliente-servidor
	

As LAN, podem caracterizar-se também quanto à sua topologia, meio de transmissão e técnicas de controlo de acesso ao meio. A topologia mais comum é a ligação em estrela (Star) sendo os diversos equipamentos ligados a um nó central, como um switch ou Access Point. Vários destes equipamentos

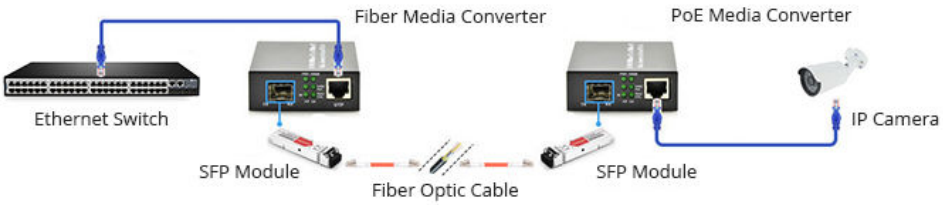
[1] Imagens: https://www.thestudygenius.com/different-types-of-networks-pan-lan-man-wan/

podem ser interligados para expandir a rede, e os meios de transmissão usados são o par trançado e a fibra ótica, também usados na topologia em anel (Ring). A thin Ethernet, 10BASE2[2] usava cabo coaxial e topologia BUS.

Quando várias LAN ou **MAN** (Rede de Área Metropolitana) são interligadas com o propósito de comunicarem entre si, formam uma WAN, interligando redes entre cidades, países ou continentes. A internet é a maior WAN mundial.



As LAN, sendo de menor dimensão que uma WAN, têm velocidades de ligação mais rápidas, maior largura de banda, são de mais fácil manutenção, embora ao nível empresarial os troços de ligação em fibra ótica, careçam de intervenção de técnicos especializados. Mesmo a nível doméstico, já não será complicado ou caro criar um pequeno troço de fibra, entre a casa e a garagem por exemplo, recorrendo a conversores fibra-RJ45 (xBASE-TX <–> xBASE-FX) [3], ou a um switch que integre as duas tecnologias.



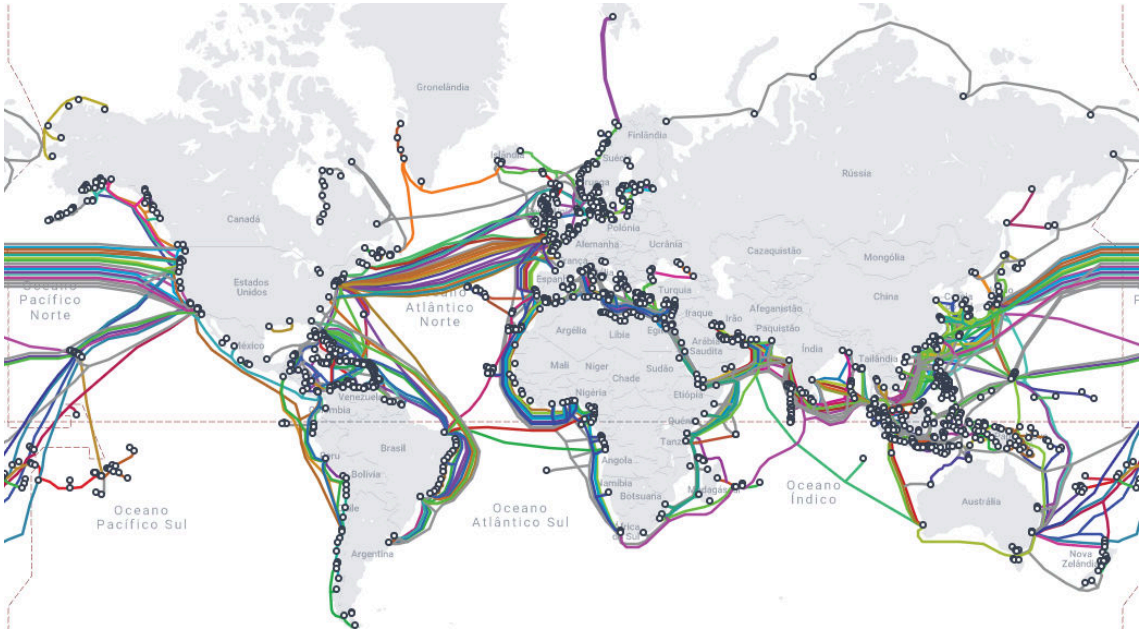
[2] https://en.wikipedia.org/wiki/10BASE2
[3] Imagens e consulta: https://community.fs.com/blog/how-fiber-media-converter-works.html

As WAN, pela sua dimensão, são difíceis de gerir e têm custos muito elevados, estando essa gestão a cargo de diversas entidades (governamentais ou privadas), que de alguma forma têm que garantir a capacidade de interligação entre diferentes tipos de redes, tecnologias, e meios de transmissão. Uma WAN interliga sub-redes de menor dimensão, como LANs, e empresas para estabelecerem ligações através da WAN podem recorrer ao aluguer de linhas dedicadas, a um provedor de serviço de rede, ou tirando partido da infraestrutura da Internet, usar VPNs (Virtual Privat Network).

Nota: A 6ª edição do livro "Computer Networks – Tannenbaum" dá a WiMAX (IEEE 802.16) como em extinção, usada para estabelecer ligações MAN, tendo perdido o passo em relação ao sistema de comunicação móvel 4G (5G), mas ainda haverá no ativo cerca de 180 operadores 802.16[4]

As ligações de rede podem ter como meio de transmissão o fio de cobre, cabo coaxial, fibra ótica e ligações de rádio, embora para WAN as duas últimas opções sejam predominantes, destacando ligações intercontinentais de fibra ótica submarina e satélite[5], como por exemplo e sistema Starlink[6]

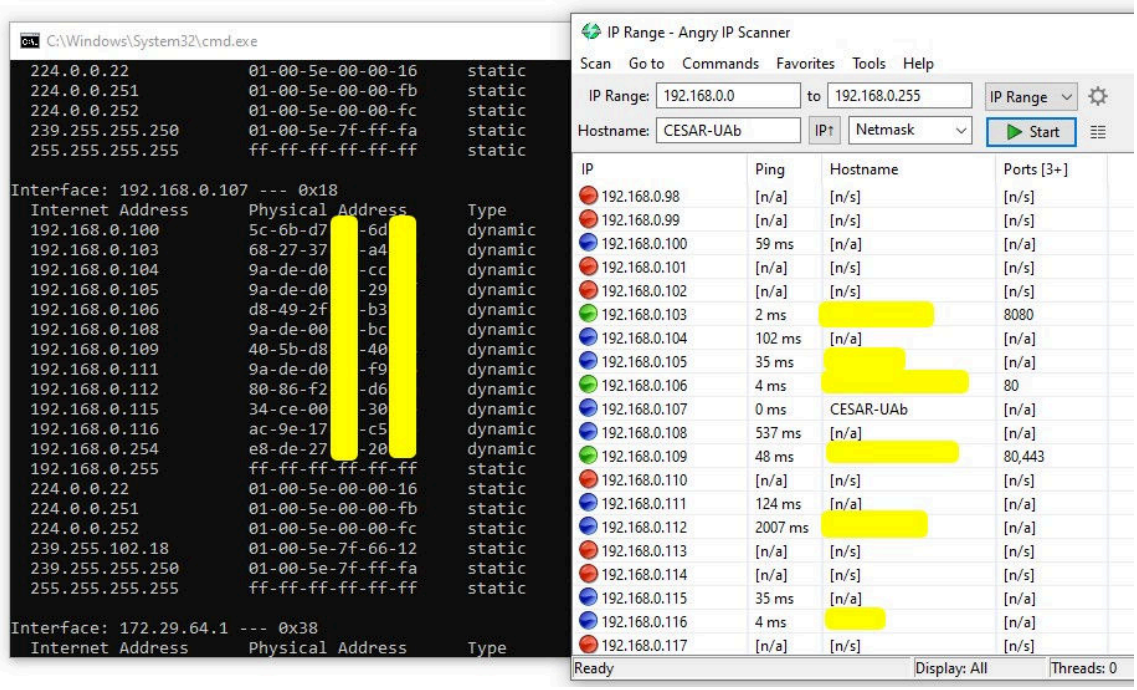
Mapa de cablagem submarina[7]



[4] https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries
[5] https://platform.leolabs.space/visualizations/leo
[6] https://pt.wikipedia.org/wiki/Starlink
[7] https://www.submarinecablemap.com/

2) **ARP** [8] [9] (Adress Protocol Resolution) é um protocolo que se destina a mapear de forma automática endereços IP da rede LAN com os endereços MAC das máquinas físicas., ou seja, traduz os endereços IP de 32 bits da camada de rede (Layer 3), nos endereços MAC de 48 bits da camada (Layer 2) de enlace de dados, estabelecendo uma ponte entre as camadas 2 e 3.

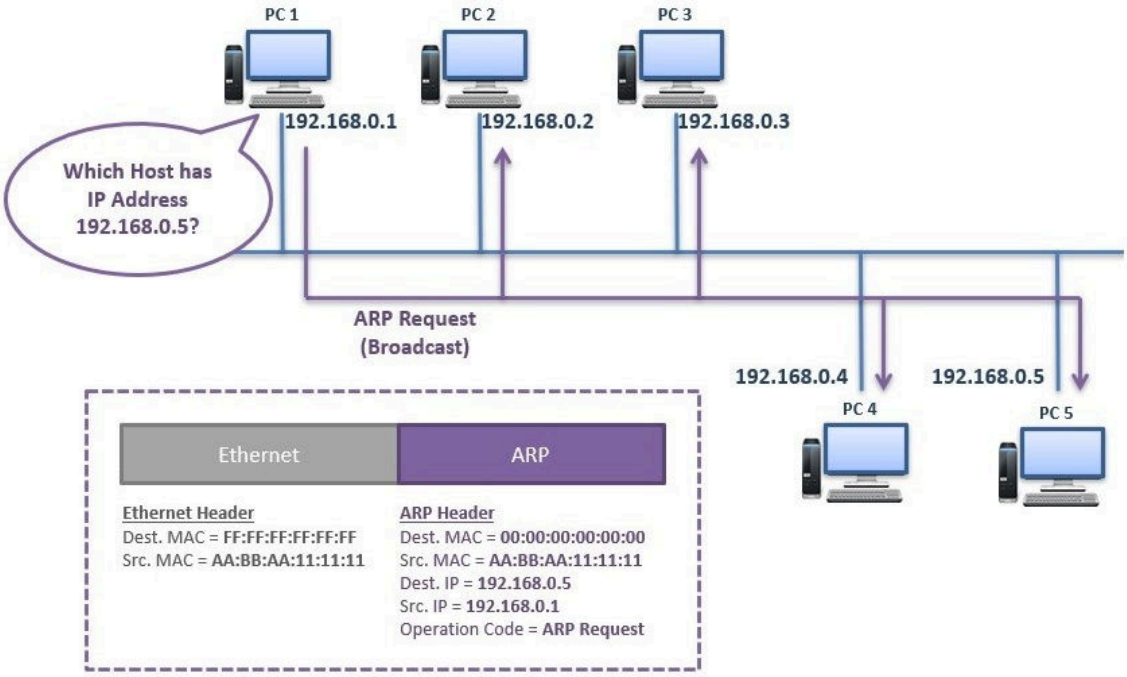
Em Windows, na linha de comandos, executando o comando ***arp -a*** serão listadas todas as entradas da tabela ARP.



Antes de um pacote IP poder ser enviado na rede, é necessário saber o endereço MAC do destinatário. Uma interface de rede (NIC) só envia e recebe frames baseados nos endereços MAC de 48bits (layer2), e não sabe nada sobre endereços IP de 32bits (layer3) para poder lidar com pacotes. Assim, se o PC que pretende enviar o pacote IP, não tiver na sua cache ARP o endereço MAC do destinatário, faz o broadcast (para todos) de um pacote ARP-discovery. Todos os dispositivos na rede recebem a requisição, que será descartada por todos, menos pelo destinatário, que responderá com um pacote unicast (para um) ARP-reply, dirigido naturalmente ao PC (emissor) que o requisitou. O PC emissor atualiza a sua cache ARP e pode então começar a enviar pacotes IP ao PC destinatário.

[8] https://www.techtarget.com/searchnetworking/definition/Address-Resolution-Protocol-ARP
[9] https://ipcisco.com/lesson/address-resolution-protocol-arp/

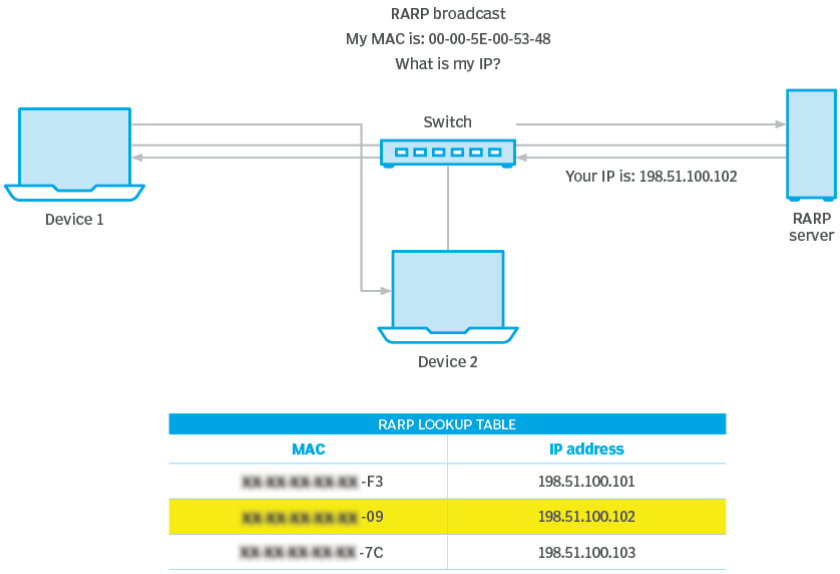
É claro que a informação (payload) colocada em frames, no processo de envio, ainda desce à camada física (layer1) para a NIC enviar os bits (0 e 1) pelo meio de transmissão, mas para a análise aqui pretendida basta considerar o caminho virtual[10] (***Emissor:*** *Layer3(IP); Layer2(MAC)* → ***Recetor****: Layer2(MAC); Layer3(IP)*) para troca de pacotes IP entre 2 dispositivos de rede.



No livro recomendado (Computer Networks 5ed, Tanenbaum,pag 467…469) encontra-se um exemplo sobre como o protocolo ARP funciona, quando dois hosts (PCs) se encontram na mesma rede (descrito no parágrafo anterior), em duas redes interligadas por um router, e no caso em que não é pretendido que o host emissor não saiba que o destinatário está numa rede distinta, sendo o router a responder ao emissor como seu endereço MAC, assumindo o encaminhamento dos frames para a rede destino. Esta solução é designada por Proxy ARP[11]. Existem outras soluções ARP[12] como gratuitous-ARP[13], ARP spoofing, ARP-poisoning ou ARP-probe.

[10] Ver: Computer Networks 5ed, Tanenbaum, páginas 194 e 195, figuras 1 e 2
[11] https://ipcisco.com/lesson/proxy-arp/
[12] https://www.geeksforgeeks.org/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/
[13] https://ipcisco.com/lesson/gratuitous-arp-ccie/

O **RARP**[14] (Reverse ARP) faz o inverso do ARP, e terá de existir na rede algum dispositivo que funcione como servidor RARP responsável por associar um endereço IP a um endereço MAC, como acontece quando um novo dispositivo é ligado à rede e ainda não tem IP adquirido. Essa tabela residirá num router-gateway na LAN. Quando uma nova máquina é instalada, e necessita de um endereço IP para poder comunicar na rede, envia um pacote de broadcast RARP que contém o seu endereço MAC nos campos de endereço destinados, quer ao hardware emissor, quer ao recetor. O servidor RARP responde a esse tipo de broadcast, procurando na tabela uma correspondência IP para MAC válida, e se existir é enviado um pacote de resposta ao requerente, contendo o endereço IP que lhe está destinado.



Alternativamente ao RARP para permitir o encaminhamento de pacotes IP, os sistemas de rede podem recorrer a protocolos de camadas superiores como a um servidor DHCP[15], serviço providenciado por exemplo por um servidor de domínio, ou ao nível doméstico pelo router do ISP. Este protocolo atribui IPs de forma dinâmica aos dispositivos que se ligam à rede (se não tiver IP fixo configurado). Similarmente um servidor de DNS na rede, mantém numa tabela[16] (forward lookup zone) uma associação de nomes dos PCs ao IP, e outra tabela inversa (reverse lookup zone) IP versus nome do PC, um pouco à semelhança do que acontece com o ARP e RARP, com IPs versus MACs.

[14] https://www.techtarget.com/searchnetworking/definition/Reverse-Address-Resolution-Protocol
[15] https://ipwithease.com/dhcp-vs-rarp/
[16] https://www.mustbegeek.com/understanding-forward-and-reverse-lookup-zones-in-dns/

3.a) O algoritmo estático flooding é usado por routers na tomada de decisões para encaminhamento de pacotes na sua vizinhança, enviando um pacote de entrada para todos as ligações de saída, exceto para aquela por onde chegou o pacote.

Pela simplicidade de configuração e robustez, porque o router apenas tem de conhecer a vizinhança e porque garante que um pacote é entregue a cada nó da rede, o flooding pode ser usado como um bloco de montagem para outros algoritmos ou protocolos que são mais eficientes, mas carecem de mais configurações, como o OSPF[17] (Open Shortest Path First) usado para encontrar o melhor caminho para pacotes entre redes, ou o DVMRP[18] (Distance Vector Multicast Routing Protocol) usado para partilha de informação entre routers para facilitar o transporte de pacotes IP multicast entre redes.

Para além do multicasting de pacotes numa rede real ou virtual, o flooding também é usado por bridges, partilha de ficheiros numa rede peer-to-peer e em redes wireless onde todas as mensagens transmitidas por uma estação podem ser recebidas por todas as outras dentro do seu alcance de rádio.

O flooding pode funcionar num de três modos: flooding não controlado, flooding seletivo e flooding controlado.

No <u>flooding não controlado</u>, não há restrições e os pacotes podem "revisitar" um router por onde já tinham passado. Sem controlo, o flooding pode ser usado com fins maliciosos, por exemplo sobrecarregando uma rede através de um ataque DoS (Denial of Service).

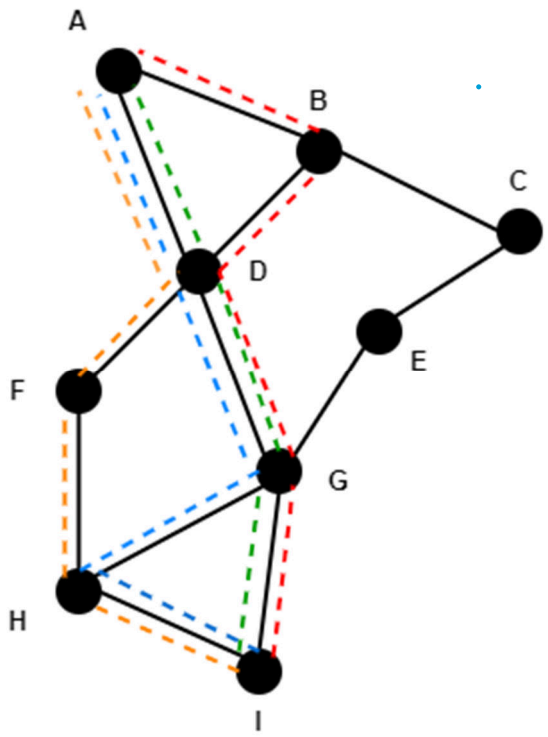
No <u>flooding seletivo</u> as ligações (ou nós) são configuradas para apenas enviar pacotes recebidos para outros routers apenas numa única direção, não sendo contudo a melhor forma de controlar o flooding.

No <u>flooding controlado</u> há dois algoritmos usados para garantir a contenção, o Reverse Path Forwarding (RPF) e o Sequence Number Controlled Flooding (SNCF). O RPF adiciona ao cabeçalho de um pacote um contador de

[17] https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First
[18] https://en.wikipedia.org/wiki/Distance_Vector_Multicast_Routing_Protocol

hops, a ser decrementado a cada hop realizado, sendo o pacote descartado quando o contador atinge zero. Idealmente o contador deve ser iniciado com o valor de hops previstos para chegar ao destino, mas pode esse valor ser o do pior cenário, por melhor garantia de sucesso na entrega. No SNCF o router insere um nº de sequência em cada pacote recebido dos seus hosts, para fazer o rastreio de pacotes transmitidos por flooding para que não sejam retransmitidos. Para tal, cada router tem de manter uma lista, por router de origem que informa sobre que números de sequência com origem num dado router já foram vistos. Para evitar um crescimento desmesurado destas listas recorre-se para cada uma a um contador K incremental, considerando que todos os números de sequência até K já foram vistos, sendo comparado o número de sequência de um pacote recebido com K para verificar se não é uma cópia, a ser descartado em caso afirmativo.

3.b) A figura[19] seguinte é uma representação da rede em apreço, com os círculos negros a representar nós (routers) e os traços que os unem a representar ligações, equivalente a hops (saltos) que um pacote terá que efetuar para passar de um nó para outro. No problema em análise um pacote terá como origem o nó A e destino o nó I, pretendendo obter-se todas as rotas possíveis com um máximo de 4 hops.



Rotas possíveis para ir da origem A ao destino I com um máximo de 4 hops:

- - - - A → D → G → I (3 hops)

- - - - A → D → G → H → I (4 hops)

- - - - A → D → F → H → I (4 hops)

- - - - A → B → D → G → I (4 hops)

[19] Diagrama elaborado em https://app.diagrams.net/

Em Windows, o comando ***tracert*** (traceroute[20]) permite saber quantos hops ocorrem desde a máquina em que o comando é executado, até ao destino definido, por URL ou IP, bem como por que gateways/routers passa e o tempo de resposta.

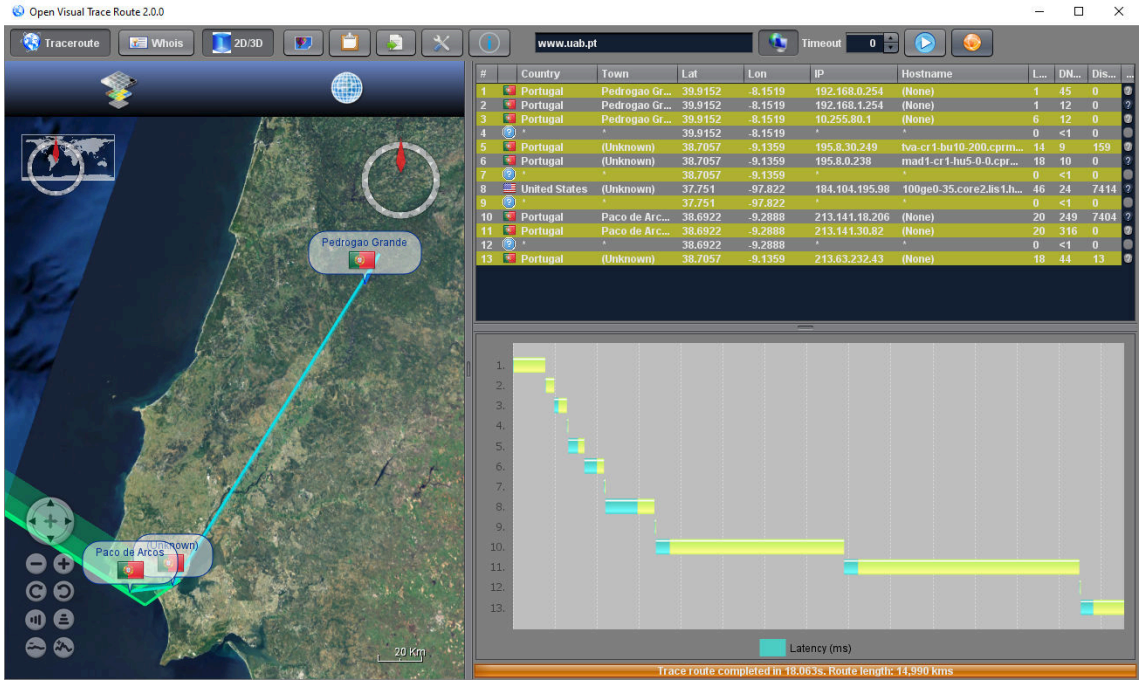
```
C:\>tracert www.uab.pt

Tracing route to uab.pt [213.63.232.43]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.254
  2     5 ms     2 ms    <1 ms  dsldevice.lan [192.168.1.254]
  3     4 ms     1 ms     3 ms  10.255.80.1
  4     *        *        *     Request timed out.
  5     8 ms     8 ms    15 ms  tva-cr1-bu10-200.cprm.net [195.8.30.249]
  6    21 ms    15 ms    15 ms  mad1-cr1-hu5-0-0.cprm.net [195.8.0.238]
  7    49 ms    47 ms     *     100ge0-36.core1.mad1.he.net [184.105.222.165]
  8    47 ms    46 ms    46 ms  100ge0-35.core2.lis1.he.net [184.104.195.98]
  9     *        *        *     Request timed out.
 10    18 ms    18 ms    18 ms  213.141.18.206
 11    18 ms    18 ms    18 ms  213.141.30.82
 12     *        *        *     Request timed out.
 13    18 ms    19 ms    18 ms  213.63.232.43

Trace complete.
```

A aplicação *Visual Trace Route*[21] permite obter resultado similar, mas com aspeto visual melhorado e informações adicionais, assinalando geograficamente as ligações que foram sendo estabelecidas.



[20] https://www.techtarget.com/whatis/definition/traceroute
[21] https://visualtraceroute.net/

4.a) Os algoritmos de roteamento dinâmico DVR (Distance Vector Routing) fazem com que cada router mantenha uma tabela (vetor) indexada a cada router da rede, contendo uma entrada para cada router, que contém duas partes: a interface de saída preferencial para o destino e uma estimativa da distância até ele. A métrica para essa distância pode ser o hop ou outra medida como por exemplo o atraso de propagação (retardo).

Se o custo de ligação entre router tiver como medida o retardo, o router pode medi-lo enviando pacotes especiais destinados aos routers na vizinhança, e que o recetor identifica com um registo de tempo e devolve o mais rápido possível.

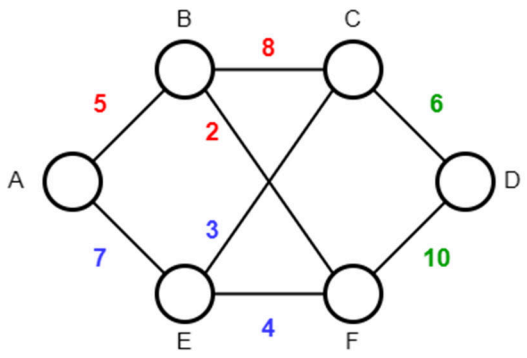
Cada router possui uma lista dos seus atrasos estimados até cada um dos outros routers na rede, enviando-a a curtos espaços de tempo aos seus vizinhos, e destes recebe listas similares, das quais se serve para atualizar a sua própria lista após soma dos valores recebidos com os existentes, construindo uma nova tabela com os menores custos de ligação obtidos para cada router, que devido a alterações na topologia da rede ou de tráfego, por exemplo, vão tendo alterados esses custos.

A convergência no cálculo para a obtenção do melhor caminho na rede com este algoritmo é relativamente rápida quando um novo router é adicionado por exemplo, mas pode ser muito lento a propagar novos valores nas tabelas quando um router é removido. O router na vizinhança imediata perde contacto com o router removido, mas continua a ter referências a caminhos válidos na sua tabela, que vai atualizando pelas que recebe de outros routers, mas que ainda “não perceberam e vão demorar a perceber” que houve um router que foi removido, e por isso há rotas que já não são válidas, mas vão sendo propagadas como existentes.

Como nota final refere-se que, o algoritmo DVR também é conhecido por Algoritmo de Roteamento Distribuído de Bellman-Ford tendo sido usado como algoritmo de roteamento original da ARPANET e também utilizado na Internet sob o nome de RIP (Routing Information Protocol).

4.b) Apresenta-se a rede com custos associados de acordo com os dados fornecidos, expostos sob forma de tabela, com cores a destacar de onde vieram os valores de custo apresentados junto de cada hop no diagrama.

		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 cálculo da nova tabela do router C, são dados do problema os novos valores do custo (retardos) para uma transmissão de C a B de 6, de C a D de 3 e de C a E de 5, pelo que falta-nos saber quais os custos mais baixos para C aceder aos routers que não estão na sua vizinhança direta, A e F.

C pode aceder a A por 3 vias: B, E e D, para o que se soma o valor do novo retardo para o hop de ligação direta a C, com o remanescente para o destino observando a tabela anterior. Temos assim que:

$$via\ B \implies CB + BA = 6 + 5 = 11$$

$$via\ E \implies CE + EA = 5 + 7 = 12$$

$$via\ D \implies CD + DA = 3 + 16 = 19$$

Assim, o caminho com menos custos para C aceder a A é via router B, com custo 11.

Executando o mesmo procedimento, calculam-se os custos das diversas rotas que C pode usar para aceder a F, podendo fazê-lo por 3 vias: B, E e D

$$via\ B \implies CB + BF = 6 + 2 = 8$$

$$via\ E \implies CE + EF = 5 + 4 = 9$$

$$via\ D \implies CD + DF = 3 + 10 = 13$$

Assim, o caminho com menos custos para C aceder a F é também via router B, com custo 8.

Apresenta-se uma tabela geral do problema, elaborada em Excel

		Origem			Retardos medidos em C			Tabela de roteamento de C	
		B	D	E	B	D	E		
					6	3	5	CUSTO	SAIDA
Destino	A	5	16	7	11	19	12	11	B
	B	0	12	6	6	15	11	6	B
	C	8	6	3	14	9	8	0	FALSO
	D	12	0	9	18	3	14	3	D
	E	6	9	0	12	12	5	5	E
	F	2	10	4	8	13	9	8	B

Bibliografia:

- Computer Networks, 5th. Edition, international;
  Tanenbaum & Wetherall; Pearson Education Limited (2014)

- Computer Networks, 6th. Edition, global;
  Tanenbaum & Wetherall; Pearson Education Limited (2021)

- Outras referências expostas em notas de rodapé ao longo do texto