

”

SISTEMAS EM REDE | 21106

A preencher pelo estudante

UNIDADE CURRICULAR: Sistemas em Rede

CÓDIGO: 21106

DOCENTE: Arnaldo Santos e Henrique São Mamede

NOME: João Paulo Alves Correia Mendes Pires

N.º DE ESTUDANTE: 2203810

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 15/12/2024

TRABALHO / RESOLUÇÃO:

Questão nº 1:

O protocolo ARP (Address Resolution Protocol) opera na interface entre as camada de rede (responsável pelo roteamento lógico através de endereços IP) e a camada de ligação de dados (responsável por gerir a comunicação através de endereços físicos MAC – media access control address) visando colmatar a necessidade de mapear endereços lógicos (IP) para endereços físicos (MAC) para permitir comunicação efetiva na rede, uma vez que os endereços físicos são únicos para cada placa de rede, tais como placas ethernet, e permitem identificar corretamente o destinatário contrariamente ao endereço IP, uma vez que uma máquina poderá possuir um ou mais endereços IP.

O funcionamento do ARP envolve a emissão de uma mensagem em broadcast chamada ARP Request, onde um dispositivo pergunta: "Quem possui este endereço IP?". Todos os dispositivos da rede recebem essa mensagem, mas apenas aquele cujo endereço IP corresponde ao solicitado responde diretamente com uma mensagem em unicast ARP Reply, fornecendo seu endereço MAC. Isso permite que o dispositivo solicitante armazene o mapeamento IP-MAC na sua tabela ARP (cache ARP) para futuras comunicações, eliminando a necessidade de consultas repetidas.

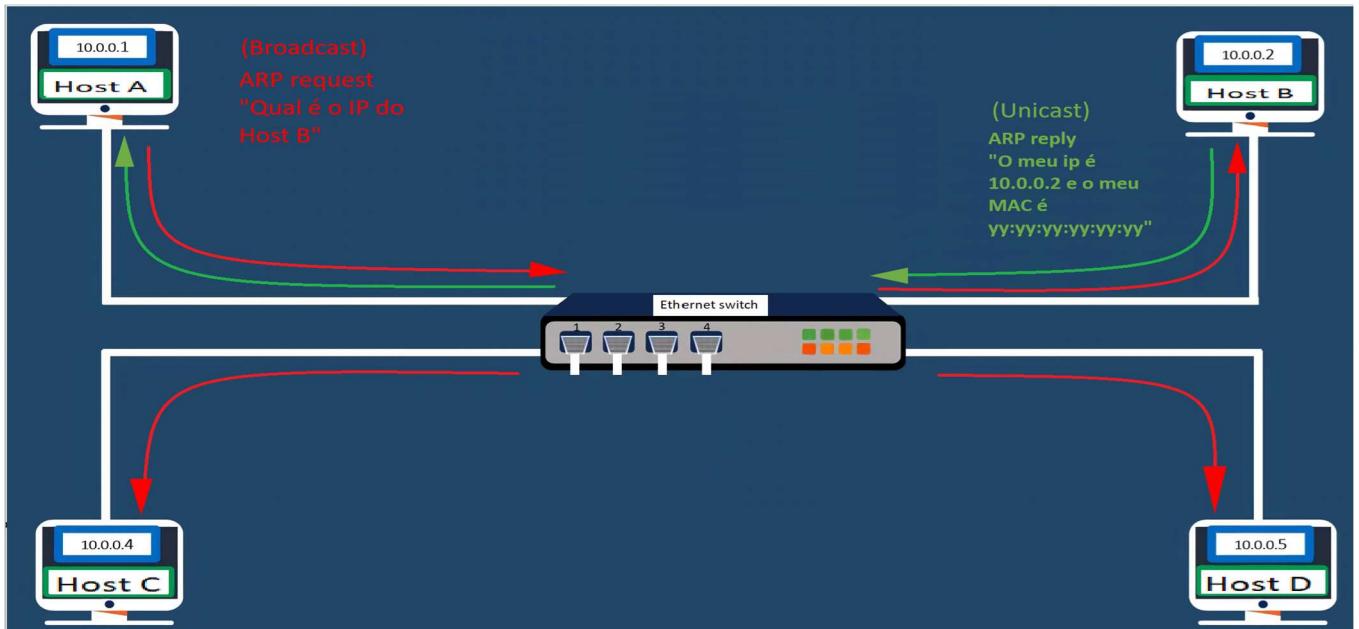
Após uma consulta bem sucedida, o pacote IP é encapsulado num frame ethernet, utilizando o endereço MAC obtido. A comunicação é estabelecida na camada de ligação de dados, enquanto os endereços IP permanecem constantes para fins de roteamento na camada de rede.

Para maior eficiência, o ARP inclui mecanismos como o armazenamento em cache, onde os dispositivos mantêm os mapeamentos por um curto período tempo, e o gratuitous ARP, que permite que dispositivos quando são configurados atualizem os caches da rede ao enviar o seu próprio mapeamento IP-MAC. Este último ajuda a detetar conflitos de endereços IP, permitindo que os gestores de rede resolvam problemas antes que prejudiquem a conectividade.

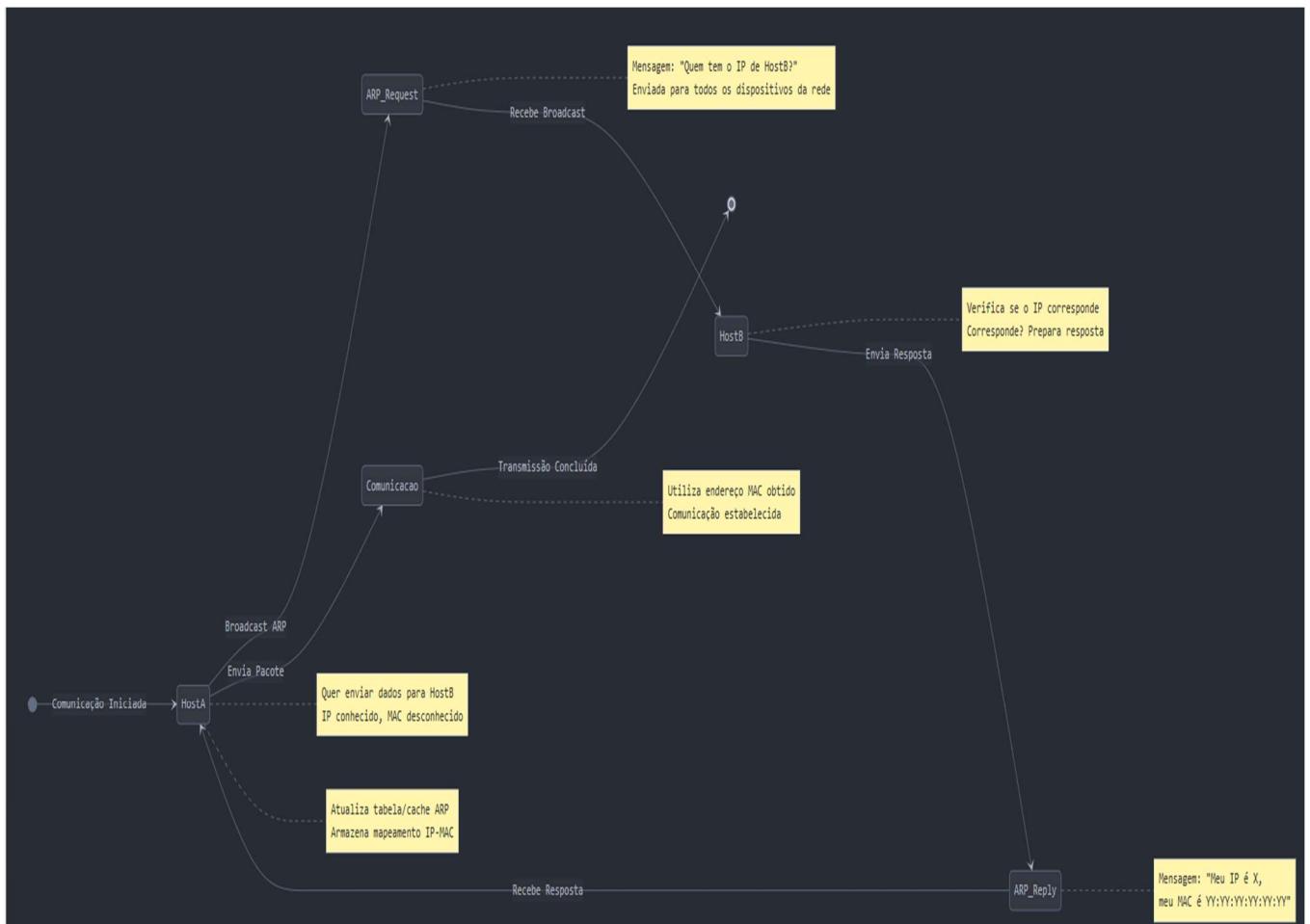
Quando o destino está fora da rede local, o dispositivo encaminha os pacotes para o router (default gateway), utilizando ARP para descobrir o endereço MAC da interface do router. O router, por sua vez, usa o ARP para

determinar o endereço MAC do próximo salto, repetindo o processo até que o pacote alcance seu destino.

Diagrama de rede:



Funcionamento:



Questão nº 2:

O formato de uma Frame Ethernet (802.3 standard) é demonstrado na seguinte figura :

Frame Ethernet (802.3 standard)								
Bytes	8	6	6	2	0 - 1500	0 - 46	4	
	Preamble	S O F	Destination Address	Source Address	Length	Data	Pad	Check-sum

IEEE 802.3, popularmente conhecida como Ethernet, é o tipo de rede local com fios mais comum um formato de frame próprio, e foi estandardizado em 1983.

A frame é composta por:

- Preâmbulo – Tem 8 bytes, cada um contendo o padrão de bits 10101010, exceto o último byte no qual os últimos 2 bits são 11. Este último byte é chamado Start Of Frame delimiter (indicado pela sigla SOF na figura do frame). Os últimos dois bits 1 indicam ao receptor que o resto do frame está prestes a começar.
- Destination Address – Tem 6 bytes, o seu primeiro bit é 0 para endereços comuns e 1 para endereços de grupo. Quando é utilizado um endereço de grupo todas as estações desse grupo recebem o frame de um único endereço, esta situação configura o conceito de *multicasting*. É, também, possível utilizar como endereço de destino todos os bits com o valor 1, reservado para *broadcasting*, o que quer dizer que o frame será aceite por todas as estações da rede.
- Source Address – Tem 6 bytes, e é um endereço único atribuído globalmente a cada estação pelo IEEE (Institute of Electrical and Electronics Engineers) e pelos fabricantes a cada placa de rede. Os primeiros 3 bytes consistem num OUI (Organizationally Unique Identifier) que indica um fabricante, e os fabricantes atribuem os últimos 3 bytes.
- Length – Tem 2 bytes, este campo é interpretado como comprimento da frame se for menor ou igual a 0x600 (1536), se for maior é interpretado como Tipo (Type).
- Data – Tem o limite máximo de 1500 bytes, e é neste campo que se insere a mensagem a transmitir ao receptor.

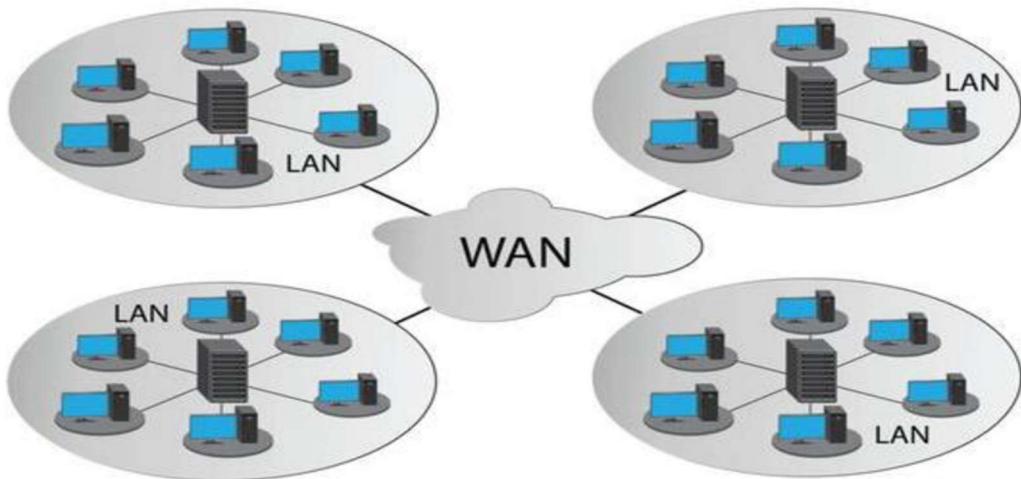
- Pad – Pode ter até 46 bytes, e tem como razão de existir o facto de existir um tamanho mínimo de frame de 64 bytes do endereço de destino até à soma de verificação, incluindo ambos. $(6+6+2+0+46+4=64)$ Pelo que se a parte dos dados for menor que 46 bytes é utilizado o campo Pad para preencher o resto do frame até ao tamanho mínimo.
- Check-sum - Tem 4 bytes, e neste campo é feita a soma de controlo. É usado o método CRC de 32 bits (cyclic redundancy check) para verificar se a frame foi recebida corretamente, caso isto não se verifique a frame é rejeitada.

Questão nº 3:

Uma LAN (Local Area Network ou Rede Local) é uma rede de computadores que abrange uma área geográfica pequena, como uma casa, um escritório ou um edifício. As LANs são tipicamente usadas para conectar computadores pessoais, workstations e servidores uns aos outros, bem como a outros dispositivos de rede, tais como impressoras e scanners, para partilha de recursos e troca de informação. As LANs são normalmente de propriedade privada e operadas por um único indivíduo ou organização.

Uma WAN (Wide Area Network ou Rede de Área Ampla) é um tipo de rede de computadores que interliga dispositivos e redes locais (LANs) em áreas geográficas vastas, como cidades, países ou até continentes. A WAN conecta sistemas dispersos em grandes distâncias, permitindo a comunicação entre dispositivos que não estão fisicamente próximos. Esta rede geralmente tem na sua composição dispositivos finais, como computadores ou servidores, que executam aplicações e interagem diretamente com os utilizadores (hosts) e switches e linhas de transmissão (sub-rede).

Uma característica importante das WANs é que sua infraestrutura geralmente é partilhada ou gerida por várias entidades, como operadoras de telecomunicações, que fornecem os meios para transmitir dados. Este tipo de rede é amplamente utilizado em empresas, governos e prestadores de serviços para possibilitar o acesso remoto, a partilha de informações e a comunicação global, na medida em que podem utilizar tipos distintos de tecnologia de rede.



Fonte: <https://www.shiksha.com/>

As LANs sem fios comparativamente a LANs com fios apresentam as seguintes vantagens e desvantagens:

Vantagens

- **Mobilidade:** As LANs sem fios permitem que os utilizadores se liguem à rede a partir de qualquer lugar dentro do alcance da rede, sem necessidade de estarem fisicamente ligados a um cabo. Isto é especialmente útil para dispositivos móveis, tais como computadores portáteis, tablets e smartphones.
- **Facilidade de instalação:** As LANs sem fios são geralmente mais fáceis de instalar do que as LANs com fios, uma vez que não requerem a instalação de cabos. Isto pode economizar tempo e dinheiro, especialmente em edifícios antigos ou onde é difícil ou caro instalar cabos.

Desvantagens

- **Segurança:** As LANs sem fios são geralmente menos seguras do que as LANs com fios porque os sinais sem fios podem ser interceptados por terceiros não autorizados. Embora existam mecanismos de segurança para proteger as LANs sem fios, tais como a encriptação WEP e WPA, estas podem não ser tão eficazes como as medidas de segurança que podem ser implementadas numa LAN com fios.
- **Desempenho:** As LANs sem fios são geralmente mais lentas do que as LANs com fios. Isto deve-se ao facto de os sinais sem fios estarem sujeitos a

interferências de outros dispositivos sem fios, bem como de objetos físicos, tais como paredes e móveis.

Questão nº 4:

a) O algoritmo de inundação (flooding) é uma técnica de roteamento estático caracterizada pela propagação de pacotes para todos os nós conectados, com exceção do nó de origem. Ou seja:

- Um nó recebe um pacote para transmissão;
- Encaminha o pacote para todos os seus vizinhos conectados;
- Cada nó repete o processo de encaminhamento.

Esta técnica implica que existe uma grande quantidade de pacotes duplicados, uma vez que se propaga por todos os caminhos possíveis, mas garante a entrega dos pacotes.

De evitar um número infinito de pacotes, que causaria inundação nos nós e nos canais de comunicação, resultando em loops e desperdício de largura de banda, são aplicadas as seguintes regras de controlo:

TTL (Time-To-Live):

- Cada pacote é enviado com um contador de "tempo de vida" (TTL);
- O contador TTL deverá ser iniciado com o número de hops necessário da origem até ao destino, caso não exista esse conhecimento deve ser considerado o pior caso possível que no qual o contador deve ser iniciado com o número que cobre toda a rede/sub-rede;
- A cada nó que o pacote atravessa, o valor do TTL é reduzido em 1.
- Quando o TTL chega a 0, o pacote é descartado, evitando loops infinitos.

Identificação de Pacotes Duplicados:

- O nó de origem coloca um número de sequência em cada pacote que recebe de seus hosts;
- Cada nó mantém um registo dos pacotes que já recebeu e descarta os pacotes duplicados para evitar retransmissões desnecessárias.

Apesar da sua ineficiência para o envio da maioria dos pacotes, o flooding tem alguns usos importantes:

Transmissão de informação (broadcasting): O flooding garante a entrega a todos os nós, o que é útil para broadcasting.

Robustez: Mesmo com a perda de vários routers, o flooding encontra um caminho se este existir, assim como a topologia de rede.

Simplicidade: Requer pouca configuração, pois os routers apenas precisam conhecer os seus vizinhos.

Ponto de referência: O flooding serve como um ponto de referência para comparar a eficiência de outros algoritmos de roteamento.

b) As rotas que o pacote seguirá são ACDEGH, ACDEFH, ABDEGH e ABDEFH.

São consumidos 9 hops de largura de banda para testar as rotas mencionadas, que é o número de possibilidades de saída de cada um dos nós desde a origem até ao destino.

Questão nº 5:

a) O Algoritmo de Vetor-Distância, também designado como Algoritmo de Roteamento Distribuído Bellman-Ford originalmente presente na ARPANET, implementa um mecanismo descentralizado para calcular o caminho mais curto entre nós em uma rede. O funcionamento deste algoritmo baseia-se num processo onde cada router mantém em memória uma tabela de roteamento que contem as linhas de saída preferidas e o vetor de distância para cada nó, que podem ser medidos pelo número de hops, pelo valor de atraso, ou outra métrica considerada mais pertinente, também designados como custos.

O inicialmente cada router apenas conhece a distância para si mesmo (zero), enviando esse vetor inicial aos routers vizinhos. Ao receberem os vetores, os routers calculam os custos de interconexão e trocam informações sobre as distâncias para os demais nós da rede.

O processo de atualização ocorre através de uma abordagem iterativa, onde os routers analisam os vetores recebidos, somam os custos de interconexão e selecionam os caminhos com menor custo total. Essas atualizações são realizadas periodicamente, geralmente entre 30 e 90 segundos, garantindo uma visão da topologia da rede. O estabelecimento das melhores rotas entre redes é chamado de convergência.

No entanto, o algoritmo apresenta uma limitação conhecida como "problema de contagem ao infinito". Esta vulnerabilidade surge devido à natureza assíncrona

das comunicações e à forma como os routers partilham informações apenas sobre custos, não sobre os caminhos específicos.

Quando ocorre uma falha em um nó, os routers continuam inicialmente a propagar informações como se o nó estivesse funcional. Esta propagação de dados incorretos pode continuar indefinidamente, sendo interrompida apenas quando um limite de custo/distância predefinido é atingido, momento em que os routers são forçados a reconstruir completamente seus vetores de roteamento.

Esta característica torna o algoritmo menos eficiente em redes grandes ou com topologias complexas, onde a deteção e recuperação de falhas podem ser significativamente lentas.

b) O roteador C recebeu as seguintes tabelas de roteamento:

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

Para calcular as distâncias (retardo) para cada router e determinar a linha de saída a usar, soma-se o vetor mais o retardo vindo de cada router:

Routers	Vetores B	Vetores + retardo B	Vetores D	Vetores + retardo D	Vetores E	Vetores + 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

Para que o router C crie uma tabela para enviar aos seus vizinhos, são selecionadas as distâncias mais curtas (marcadas a verde) para cada um dos routers, resultando a seguinte tabela:

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

De acordo com o cálculo constante na tabela o vetor transmitido é

C: (11, 6, -, 3, 5, 8).

Referências bibliográficas:

Tanenbaum, A. S., Wetherall, D.J. Computer Networks. 6th Edition, Pearson
New International Edition, USA

Slides de apoio, Fórum UC – Sistemas em Rede

<https://www.shiksha.com/>