E-fólio Global | Folha de resolução do E-fólio

UNIDADE CURRICULAR: Sistemas em Rede

CÓDIGO: 21106

DOCENTE: Arnaldo Santos

A preencher pelo estudante

NOME: Júlio César Gomes de Barros

N.º DE ESTUDANTE: 1902295

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 2 fevereiro 2023

TRABALHO / RESOLUÇÃO:

1) Vantagens da LAN sem fios

Desde logo a mobilidade. A possibilidade de ligar e remover um equipamento da rede, como um portátil ou outro equipamento móvel.

É mais fácil de expandir, pois pode bastar adicionar mais um AccessPoint ou repetidor, sem necessidade passar cablagem que encarece tipicamente os custos e levanta algumas dificuldades físicas.

Desvantagens da LAN sem fios

Devido à portabilidade, os equipamentos funcionam tipicamente a baterias, pelo que é necessário que tenham de ser carregados com alguma regularidade, e podem produzir-se falhas de comunicação.

As velocidades de ligação são tipicamente mais lentas, e a propensão para colisões e congestionamentos nas comunicações aumenta com a expansão da rede.

A segurança, pois com ligações a cabo será mais difícil aceder de forma indevida á rede, do que o é conseguir acesso a sinais rádio.

2) O conceito de provisioning (provisionamento) concerne á prevenção e possibilidade de ser necessário acomodar recursos extra a uma rede, de preferência de forma dinâmica, caso ocorram congestionamentos. Por exemplo, switch e/ou routers com portas disponíveis para acomodar novos serviços, possibilidades de expansão da rede, ligações a mais servidores, ou eventualmente neste adicionar mais discos. Possibilidade de upgrade de tecnologias como interligação a redes de fibra-óptica, aquisição de maior largura de banda para conexões ao exterior. A concento baseia-se na premissa de que a tecnologia está em permanente desenvolvimento e carece de atualizações que não será possível realizar em grande escala e de uma só vez, pelo que se

vai acautelando potenciais vias de upgrade, considerando os equipamentos que estão mais sujeitos a congestionar a rede e serviços.

3) O DHCP (Dynamic Host Configuration Protocol) é um protocolo destinado a atribuir IPs dinamicamente a hosts. O DHCP necessita de um servidor, que deve ser único na rede, ou havendo mais do que um, devem ter pools (gama de endereços) de atribuição de IPs distintas para não criar conflitos (atribuição do mesmo IP a pelo menos 2 hosts na rede).

Quando um host se liga numa rede ele não possui mais do que o MAC address, mas para comunicar da camada de rede necessita de um IP, pelo que faz um Broadcast na rede solicitando um IP, usando um pacote DHCP discover. Havendo um servidor DHCP na rede, este disponibiliza um IP disponível na sua pool de IPs e envia um pacote DHCP offer ao host, identificando o host pelo endereço Ethernet que constava no pacote DHCP discover.

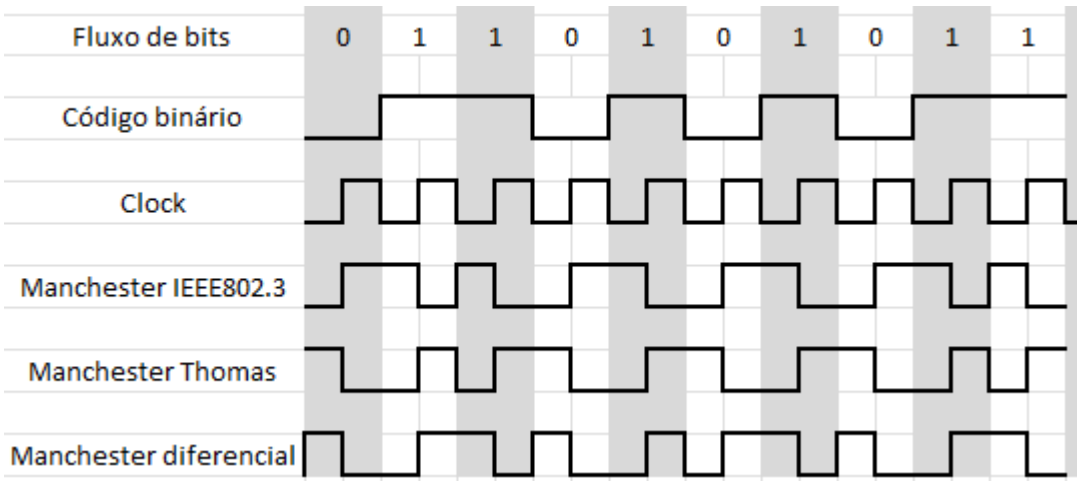
4) Os fluxos de bytes confiável (exemplo: sequência de páginas de um livro) e fluxo de mensagens confiável (exemplo: download de um filme) são distintos, pois neste último caso a rede mantém um controlo sobre a dimensão da mensagem, e tal não acontece no caso do fluxo de bytes.

No caso do download de um filme, a mensagem, que é o filme, é dividida em pacotes a ser entregues num dado destino, e cada um deles conterá informação sobre que parte da mensagem transporta, e no fim todos os pacotes são recompostos para compor a mensagem final, independentemente da ordem por que chegaram. A informação sobre a mensagem não se perde.

No caso do envio de páginas de um livro, como se fosse um fluxo de bytes, não há informação sobre a ordem pela qual se enviam nem como devem ser ordenados, ou se algum pacote se perdeu.

5) Sim, há sempre a possibilidade de ocorrerem erros, nomeadamente em caso de perturbação severa, por exemplo em cablagem de cobre de comunicação de dados que circule nas proximidades de linhas de energia. Uma quantidade significativa de ruído pode não ser possível de corrigir por códigos de correção de erros, ou até de detetar, no infortúnio de os erros introduzidos serem adulterados de tal forma que que por exemplo, um dado com correção de paridade par, dado com tal, ter 2 bits invertidos e continuar a ser par. Tal pode perfeitamente ocorrer com o endereço de destino inscrito num pacote de dados, que adulterado pode tomar outro rumo.

6) Representação da codificação Manchester IEEE802 (XOR com clock), Manchester G. E. Thomas (XNOR com clock) e Manchester diferencial, onde um 0 produz transição imediata do estado anterior, e um 1 mantém o estado até à inversão a meio do bit que caracteriza as variantes de codificação Manchester.



7) O router implementa o CIDR (Classless Inter-Domain Routing) como sub-redes para os prefixos dados /22 e /23

Block ID = 22
Host ID = 32
Subnet: 10 bits (32-22) para subnet
Mask: 255.255.252.0

Block ID = 23
Host ID = 32
Subnet: 9 bits (32-23) para subnet
Mask: 255.255.254.0

De acordo com a tabela de entradas CIDR, convertendo o IP para binário e o prefixo definindo o nº de 1s a alinhar á esquerda para a sub-rede, definindo a máscara, realiza-se um E lógico bit a bit para obter a Net ID.

Endreço/prefixo	Próximo hop	Primeiro IP	Último IP
145.48.56.0/22	Interface 0	145.48.56.1	145.48.59.254
145.48.60.0/22	Interface 1	145.48.60.1	145.48.63.254
192.54.40.0/23	Router 1	192.54.40.1	192.54.41.254
default	Router 2		

7.a) Para o IP de entrada 145.48.63.10 temos

		Endereço IP				/prefixo	
Host ID	IPv4 32 bits	145	48	63	10	22	← INPUT
		1 0 0 1 0 0 0 1	0 0 1 1 0 0 0 0	0 0 1 1 1 1 1 1	0 0 0 0 1 0 1 0	10110	
Subnet	10	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 0 0	0 0 0 0 0 0 0 0	1024	Dimensão da Subnet
Máscara		255	255	252	0		
Net ID	IP	1 0 0 1 0 0 0 1	0 0 1 1 0 0 0 0	0 0 1 1 1 1 0 0	0 0 0 0 0 0 0 0		
		145	48	60	0		
Subnet inverso (Cisco wildcard mask)		0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1	1 1 1 1 1 1 1 1		
		0	0	3	255		
Network ID		145	48	60	0		
Primeiro IP		145	48	60	1	Hosts disponíveis	
Último IP		145	48	63	254	1022	
Broadcast		145	48	63	255		

Como o IP 145.48.63.10 está dentro do endereço/prefixo 145.48.60.0/22 fará o hop para o Interface 1

7.b) Para o IP de entrada 192.54.40.7 temos

		Endereço IP				/prefixo	
Host ID	IPv4 32 bits	192	54	40	7	23	← INPUT
		1 1 0 0 0 0 0 0	0 0 1 1 0 1 1 0	0 0 1 0 1 0 0 0	0 0 0 0 0 1 1 1	10111	
Subnet	9	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 0	0 0 0 0 0 0 0 0	512	Dimensão da Subnet
Máscara		255	255	254	0		
Net ID	IP	1 1 0 0 0 0 0 0	0 0 1 1 0 1 1 0	0 0 1 0 1 0 0 0	0 0 0 0 0 0 0 0		
		192	54	40	0		
Subnet inverso (Cisco wildcard mask)		0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	1 1 1 1 1 1 1 1		
		0	0	1	255		
Network ID		192	54	40	0		
Primeiro IP		192	54	40	1	Hosts disponíveis	
Último IP		192	54	41	254	510	
Broadcast		192	54	41	255		

Como o IP 192.54.40.7 está dentro do endereço/prefixo 192.54.40.0 /23 fará o hop para o Router 1.

8.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.

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

Como o algoritmo foolding gera uma infinidade de pacotes duplicados, na variante controlada para garantir a contenção, adiciona ao cabeçalho do pacote um contador de hops (transição ou salto, entre dispositivos de rede), a ser decrementado a cada hop realizado, sendo o pacote descartado quando atinge zero. Idealmente o contador deve ser iniciado com o valor de hops previstos para chegar ao destino, mas se o remetente não souber a extensão do caminho, pode iniciar o contador com o valor para o pior cenário (diâmetro total da rede ou sub-rede), por melhor garantia de sucesso na entrega.

8.b)

Com máximo de 5 hops as rotas possíveis são: A-C-D-E-G-H, A-C-D-E-F-H, A-B-D-E-F-H e A-B-D-E-G-H

Consome 9 hops de largura de banda para testar todas as rotas, que é o nº total de possibilidades de saída de cada um dos nós.

Bibliografia: *Computer Networks 5th edition, Tanenbaum*