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

UNIDADE CURRICULAR: Sistemas de Rede

CÓDIGO: 21106

DOCENTE: Arnaldo Santos

A preencher pelo estudante

NOME: Ivo Vieira Baptista

N.º DE ESTUDANTE: 2100927

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 02-02-2022

TRABALHO / RESOLUÇÃO:

Resposta 1)

Vantagens da LAN sem fios (Wireless):

Mobilidade: Uma das principais vantagens da LAN sem fios é a mobilidade. Com uma rede sem fios, os dispositivos podem se conectar à rede em qualquer lugar dentro da área de cobertura sem fios, o que é ideal para dispositivos móveis como laptops e smartphones.

Fácil instalação: Uma outra vantagem é a facilidade de instalação. Não é necessário instalar cabos para cada dispositivo, o que pode ser um processo trabalhoso e caro em uma rede com fios.

Desvantagens da LAN sem fios (Wireless):

Instabilidade: Uma das principais desvantagens da LAN sem fios é a instabilidade da conexão. As condições ambientais, como obstáculos ou interferências de outras redes sem fios, podem afetar a qualidade da conexão.

Segurança: Outra desvantagem é a segurança. Como as redes sem fios são acessíveis a partir de qualquer lugar dentro da área de cobertura, elas podem ser mais vulneráveis a invasões de segurança, como a intercetação de dados transmitidos.

Em resumo, a LAN sem fios oferece mobilidade e facilidade de instalação, mas pode ser instável e menos segura do que uma LAN com fios. Ainda que os roteadores e hosts estejam funcionando corretamente e o software não tenha erros, existe a possibilidade de um pacote ser entregue no destino errado devido a fatores como interferências na rede, erros de rotação, congestão de tráfego ou falhas de hardware. No entanto, as taxas de erro são geralmente muito baixas e há mecanismos para detetar e corrigir erros de entrega.

Vantagens LAN sobre WAN

Mais rápidas e mais económicas por ter uma dimensão menor comparada com a WAN, o modelo LAN to LAN proporciona o grande beneficio de redução de custos, com uma rede LAN podemos compartilhar recursos facilmente com outros computadores, economizando despesas, porque não precisamos comprar mais dispositivos, como impressoras, scanners, ou dispositivos de armazenamento para cada computador, basta comprar um e compartilhar para

estes dispositivos serem acessados desde os outros computadores.

Resumindo podemos dizer que:

A LAN é mais rápida do que a WAN, pois os dispositivos estão fisicamente próximos um do outro.

A LAN é mais segura, pois os dados só viajam através de cabos físicos. A LAN é mais barata de implementar e manter do que a WAN. **Desvantagens LAN**

É a segurança mais vulnerável, problemas com um servidor central se falha ficam todos sem acesso aos dados que este tinha, como por exemplo uma aplicação de faturação.

Resumindo podemos dizer que:

A LAN é limitada geograficamente e só pode conectar dispositivos em uma área local.

A LAN não fornece acesso à Internet para todos os dispositivos conectados.

LAN com fios (fibra ou cobre)

É instrutivo comparar a fibra com o cobre. A fibra tem muitas vantagens, pois a mesma pode gerenciar larguras de banda muito mais altas do que o cobre. Esta característica sozinha já justificaria seu uso nas redes de última geração.

A fibra depende da luz em vez da eletricidade para transmitir dados, o que facilita conexões de Internet muito mais rápidas, capazes de lidar com maior largura de banda, a velocidade de download e upload é a mesma na fibra e comparado com o cobre é muito mais rápida, sendo capaz de transmitir 1 gigabit por segundo. No entanto a Fibra ótica é mais segura, tendo maior alcance, enquanto com o cobre precisamos de toneladas de cabo para dar a mesma largura de banda que o de fibra, em que as flutuações de temperatura, condições climáticas severas e humidade podem causar corrosão e perda de conectividade, no Cabo de cobre velho ou desgastado pode até apresentar um risco de incêndio, devido ao fato de que ele carrega uma corrente elétrica, por isso a fibra é mais confiável. Com o tempo, a fibra é mais cara, o investimento é maior, mas a largo prazo tem mais durabilidade, período de vida ao contrário do cobre, cuja baixa atenuação da fibra ótica permite a redução do número de repetidores o que traz uma economia de custo significativa na sua instalação. Esta apenas necessita de um repetidor a cada 50 km e os fios de cobre necessitam de um repetidor a cada 5km. Alem disso a fibra é muito mais leve que o cobre. Mil pares trançados com 1 km de comprimento pesam 8 toneladas. Duas fibras têm mais capacidade e pesam apenas 100 kg, a transmissão ótica é basicamente unidirecional, em que a comunicação bidirecional exige duas fibras ou duas bandas de frequência numa única fibra, sendo que as interfaces de fibra são mais caras que as interfaces elétricas. Apesar disso, o futuro de toda a comunicação fixa de dados para distâncias superiores a alguns metros depende claramente da fibra

Vantagens:

a) A fibra ótica é feita de fibras de vidro ou plástico, maioritariamente de Oxido de Sílica, que pertence aos materiais isolantes, não corroem ou oxidam como o cobre. Adicionalmente permite uma baixa interferência eletromagnética e/ou de picos de tensão.
b) Maior Velocidade de transmissão de dados.

Desvantagens:

a) A fibra ótica requer especialistas com conhecimentos na área, a instalação ou fusões para união de fibras(junta)e o comportamento da luz no interior da fibra (reflexão total interna).
b) A fibra ótica pode ser danificada com facilidade na sua instalação, se for dobrada a mais pode partir, ao contrário do fio de cobre que possui maior resistência ao manuseamento.

Resumindo:

Vantagens da LAN sem fios (Wireless) em comparação com uma LAN com fios (fibra ou cobre):

Mobilidade: Uma das principais vantagens de uma LAN sem fios é a mobilidade. Sem o uso de cabos, os dispositivos podem se conectar à rede a partir de qualquer local dentro do alcance da rede sem fios.

Instalação fácil: Instalar uma LAN sem fios é muito mais fácil do que instalar uma LAN com fios, pois não é necessário fazer furos nas paredes ou passar cabos por toda a casa ou escritório.

Desvantagens da LAN sem fios (Wireless) em comparação com uma LAN com fios (fibra ou cobre):

Interferências: Uma das principais desvantagens da LAN sem fios é a interferência de outros dispositivos sem fios, como telefones celulares e outras redes sem fios, o que pode resultar em uma conexão instável.

Segurança: Uma LAN sem fios pode ser mais vulnerável à invasão do que uma LAN com fios, pois os dados transmitidos sem fios podem ser intercetados por terceiros sem autorização. É importante usar medidas de segurança, como criptografia, para proteger os dados transmitidos na rede sem fios.

Resposta 2)

O provisioning consiste na alocação de recursos de rede pré-determinados para garantir que a largura de banda necessária esteja disponível para cada dispositivo ou aplicação na rede. Isto envolve a definição da capacidade da rede necessária para atender as suas exigências, de modo a evitar o congestionamento da rede. É uma abordagem básica de gerir o congestionamento, que permite assegurar que a largura de banda necessária está disponível para todas as aplicações críticas, evitando assim o congestionamento da rede.

Provisioning é o processo de alocar recursos de rede para atender as necessidades atuais e futuras de capacidade e desempenho. Isso inclui a configuração de equipamentos de rede, como roteadores e switches, e a atribuição de largura de banda para diferentes aplicações e usuários. O objetivo é garantir que a rede seja capaz de lidar com o tráfego esperado e, em caso de congestão, aumentar a capacidade adicionando mais recursos de rede.

Por exemplo, se uma empresa deteta que sua rede está sobrecarregada devido ao aumento do uso de vídeo e transferência de arquivos de grande porte, pode optar por fazer um upgrade na largura de banda das ligações de rede mais intensamente utilizadas ou adquirir mais largura de banda no mercado. Isso ajuda a garantir que a rede continue a fornecer um desempenho aceitável mesmo quando há congestão.

Resposta 3)

DHCP (Dynamic Host Configuration Protocol) é um protocolo de rede utilizado para atribuir endereços IP dinamicamente a dispositivos em uma rede. Ele permite que um dispositivo se conecte a uma rede e receba automaticamente informações de configuração de rede, como endereço IP, máscara de sub-rede, gateway padrão e servidores DNS. Isso facilita a administração da rede, já que os administradores não precisam configurar manualmente cada dispositivo e podem economizar tempo ao lidar com dispositivos adicionais ou mudanças na rede. Além disso, o DHCP ajuda a evitar conflitos de endereços IP na rede, garantindo que cada dispositivo tenha um endereço único. Por exemplo podemos colocar um router com internet na sala e com um cabo colocar outro router sem o DHCP no quarto e conseguiríamos dar WiFi ao quarto facilmente.

Resposta 4)

Não, essas duas redes não são idênticas. Embora ambas forneçam um serviço confiável orientado à ligação, a forma como fornecem esse serviço é diferente.

Uma rede que oferece um fluxo de bytes confiável (como o protocolo TCP) garante que todos os bytes transmitidos cheguem ao destinatário na ordem correta e sem erros. Ela usa um mecanismo de confirmação de recebimento e retransmissão para garantir a integridade dos dados.

Por outro lado, uma rede que oferece um fluxo de mensagens confiável (como o protocolo UDP) não garante a entrega de todos os pacotes na ordem correta ou sem erros, mas fornece uma forma de transmitir mensagens de forma confiável. Em vez de transmitir dados como um fluxo contínuo de bytes, a rede divide os dados em mensagens e as envia como pacotes separados. O destinatário reconstrói as mensagens a partir dos pacotes recebidos.

Em resumo, a principal diferença entre essas duas redes é a forma como garantem a entrega confiável dos dados. Enquanto a primeira garante a entrega de todos os bytes na ordem correta, a segunda garante a entrega das mensagens completas, mesmo que alguns pacotes possam ser perdidos ou chegar fora de ordem.

Resumindo e poucas palavras:

Não, as duas redes não são idênticas. A diferença entre um fluxo de bytes confiável e um fluxo de mensagens confiável é que, no primeiro caso, todos os bytes enviados são garantidos para chegar ao destino na ordem correta e sem perda, enquanto no segundo caso, as mensagens são enviadas e recebidas como unidades distintas, garantindo que cada mensagem chegue ao destino, mas não necessariamente na ordem em que foram enviadas.

Um exemplo de diferença entre as duas redes é que, em uma rede de fluxo de bytes confiável, se um arquivo grande é enviado e há uma falha de rede durante a transferência, a conexão é reiniciada e os bytes perdidos são reenviados, garantindo a integridade dos dados. Em uma rede de fluxo de mensagens confiável, as mensagens perdidas podem não ser reenviadas e o destinatário deve lidar com a falta de informação.

Resposta 5)

Sim, há uma hipótese de um pacote ser entregue no destino errado, mesmo quando os roteadores e hosts estão funcionando adequadamente e o software está isento de erros. Isso pode acontecer devido a uma série de fatores, como interferências na rede, erros de rotação, congestionamento de tráfego ou falhas de hardware. Além disso, a natureza distribuída da internet significa que há muitos pontos de falha potenciais ao longo do caminho de um pacote, cada um dos quais pode levar a um erro de entrega.

No entanto, as taxas de erro são geralmente muito baixas e as redes de computadores têm métodos para detetar e corrigir erros de entrega, por isso a entrega correta de pacotes é geralmente garantida. Além disso, as tecnologias de rede, como o TCP, são projetadas para lidar com erros de entrega e garantir a entrega confiável dos dados.

Resumindo, ainda que os roteadores e hosts estejam funcionando corretamente e o software não tenha erros, existe a possibilidade de um pacote ser entregue no destino errado devido a fatores como interferências na rede, erros de rotação, congestão de tráfego ou falhas de hardware. No entanto, as taxas de erro são geralmente muito baixas e há mecanismos para detetar e corrigir erros de entrega.

Resposta 6)

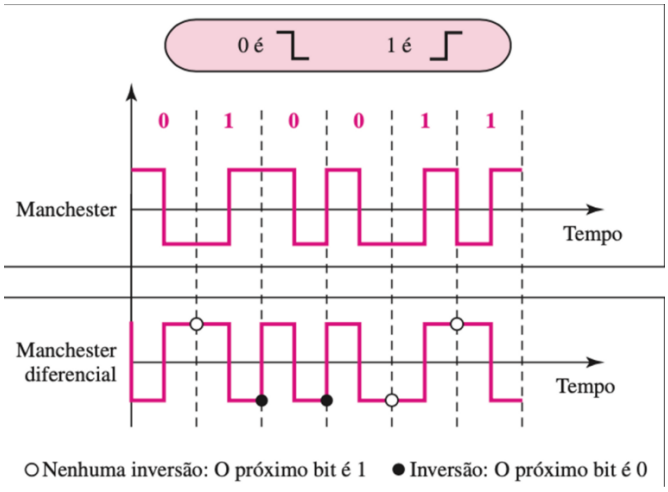
Manchester

É uma “evolução” é polar, ou seja, os níveis alto e baixo, são tensões simétricas, não é como no TTL, 0 são cerca de 0v e um 1 são cerca de 5v, mas o Manchester mete as transições a meio do bit, e assim leva com ele um clock, porque no NRZ, se temos muitos 1s ou 0s seguidos, a certa altura podes não saber já quantos são e por outro lado, ficamos com a linha muito tempo com tensão positiva ou negativa, com o Manchester está sempre a fazer saltar os valores entre positivo e negativo, o resultado é que a linha tem média de tensão 0v, ou seja, 0 volt DC.

Para mim O Manchester diferencial é só isto

0 - tem logo um transição no início

1 - não transita logo, só depois a meio do bit



Mas eu estive a investigar muito o Manchester diferencial e tem muitos sítios na internet com erros e em livros, exemplo errado:

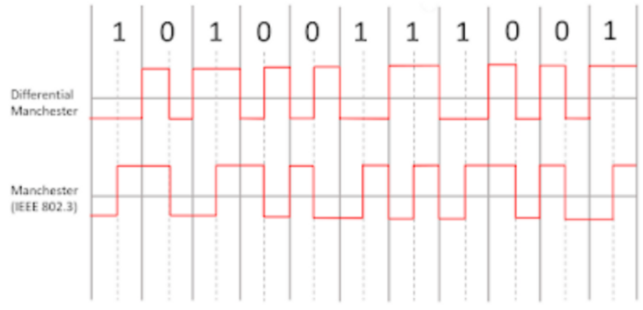


Figure 1. Differential Manchester encoding is based on the presence or absence of a transition, whereas Manchester encoding relies on the polarity of the transition.

Já sabemos que em qualquer codificação Manchester depois há as transições a meio do bit.

Este tem o diferencial errado. o 1 está sempre no mesmo estado, sem a transição a meio do bit, e aí o 1, também provoca transição no início do bit, o que está errado

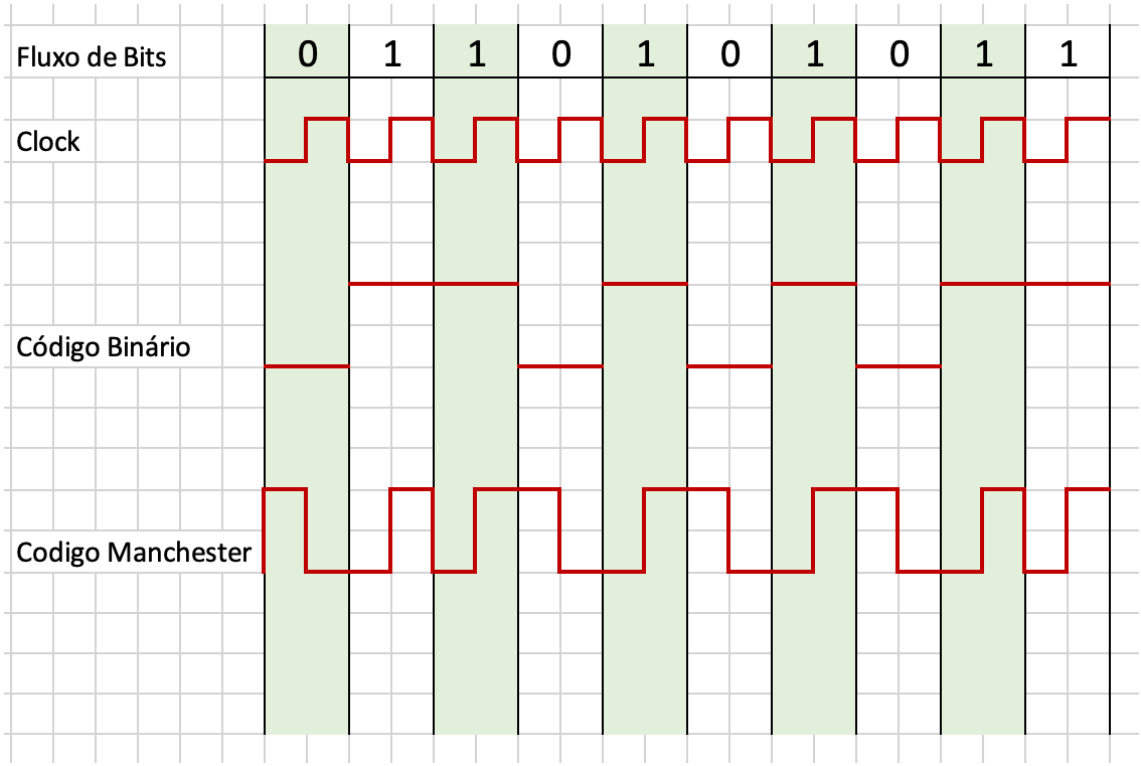
Também fiz um programa em Python, com a simulação do Manchester mas tenho erro no Manchester diferencial, estou a investigar, mas é difícil de simular, deixo aqui o link se o prof quiser testar, o Manchester esta ok com o Thomas.

http://manchester.ivo.com.pt:8502

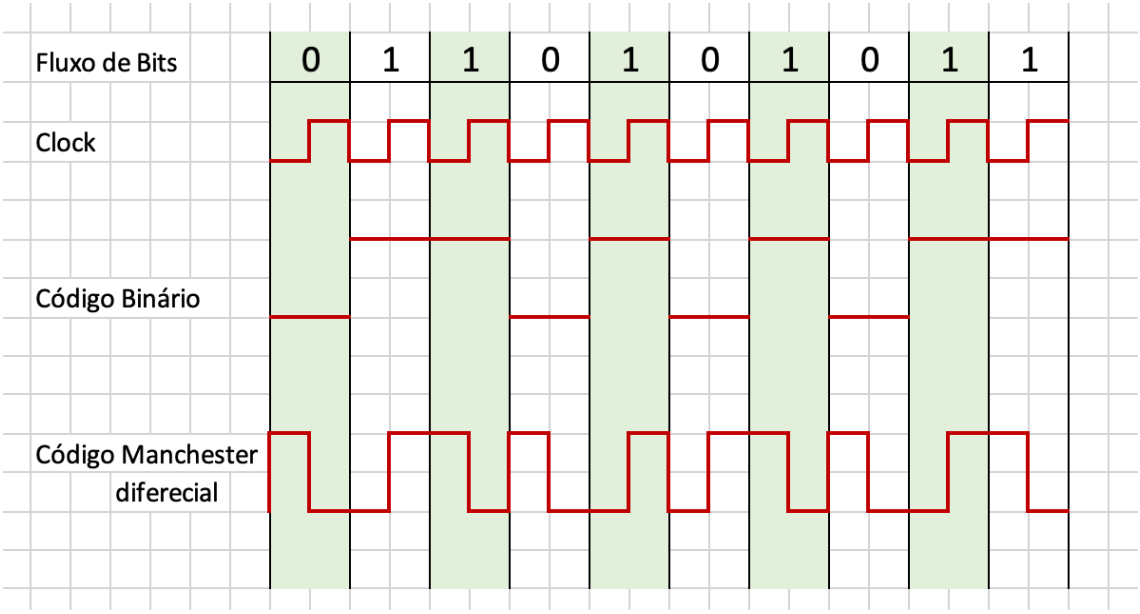
Os meus exemplos para a resposta seria os gráficos a continuação:

A codificação Manchester divide a duração do bit em duas metades, com a voltagem mantida em um nível durante a primeira metade e mudando para o outro nível na segunda metade. A transição no meio do bit fornece sincronismo. Já o método Manchester diferencial combina aspectos dos métodos RZ e NRZ-I e sempre há uma transição no meio do bit, mas seu valor é determinado no início do bit. Se o próximo bit é 0, há transição, caso contrário não há.

Codificação Manchester:



Codificação Manchester Diferencial:



Reposta 7)

O CIDR (Classless Inter-Domain Routing) é um método de atribuição de endereços IP que permite a alocação mais eficiente de endereços na Internet. Em vez de usar uma classe fixa de endereços IP (como Class A, B ou C), o CIDR permite a atribuição de blocos de endereços IP de tamanho variável a organizações ou redes, baseado na necessidade real de endereços IP. O CIDR é utilizado para reduzir a quantidade de informação de roteamento na Internet, melhorando assim a eficiência e escalabilidade do roteamento de pacotes na Internet. Agora calculando:

Blok ID = 22
Host ID = 32
Subnet: **10 bits** (32-22) para subnet Mask: **255.255.255.252**

Blok ID = 23
Host ID = 32
Subnet: **9 bits** (32-23) para subnet Mask: **255.255.255.254**

Calculamos a gama de endereços de IP e máscaras baseado nas informações de CIDR fornecidas na tabela de roteamento:

Endreço/Máscara	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		

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

		145								48								63								10							
IP address		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
/	22	1	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
		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
Net ID		145								48								60								0							

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

		192								54								40								7							
IP address		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	1	1	1
/	23	1	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
		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
Net ID		192								54								40								0							

Resposta 8)

a)

Os algoritmos de roteamento por vetor de distância operam fazendo cada roteador manter uma tabela (isto é, um vetor) que fornece a melhor distância conhecida até cada destino e determina qual enlace deve ser utilizado para chegar lá. Essas tabelas são atualizadas por meio da troca de informações com os vizinhos. No fim, cada roteador saberá o melhor enlace para alcançar cada destino. No roteamento por vetor de distância, cada roteador mantém uma tabela de roteamento indexada para cada roteador da rede e que contém uma entrada para cada um deles. Essa entrada contém duas partes: a interface de saída preferencial a ser utilizada para o destino e uma estimativa da distância até esse destino. A métrica utilizada pode ser o número de hops ou outra medida, conforme discutimos para o cálculo do caminho mais curto. O roteamento com vetor de distância ou em inglês "**Distance Vector Routing**", foi o algoritmo de roteamento original da ARPNET. É conhecido por diversos nomes, sendo o mais comum o algoritmo de roteamento distribuído de **Bellman-Ford**. Em termos comparativos, para entendimento deste processo, temos o exemplo do sistema

de navegação por GPS quando estamos em um local (origem) e pretendemos ir para um destino pelo caminho mais rápido calculando todas as possíveis estradas que irão dar ao destino considerando tráfego, outros, etc.

b)

O número de rotas são 4, com no máximo 5 hops, estes seriam os que o pacote seguira, agora a quantidade de largura de banda consumida pelo pacote dependerá de vários fatores, como o tamanho do pacote, a velocidade da rede, etc. Portanto, não é possível determinar a quantidade de largura de banda consumida sem mais informações.

CDEGH

CDEFH

BDEGH

BDEFH