1.)

O DHCP (Dynamic Host Configuration Protocol) é um protocolo que facilita a atribuição automática de endereços de IP a dispositivos em uma rede. Para que funcione, é necessário haver um servidor DHCP, que deve ser único na rede. Caso existam vários servidores DHCP, cada um deve ter uma faixa (pool) de endereços IP distinta para evitar conflitos, como dois dispositivos recebendo o mesmo endereço de IP.

Quando um dispositivo se conecta a rede, ele inicialmente só possui o seu endereço MAC (Meida Acess Control) e ainda não tem um endereço de IP, para o obter o dispositivo envia um pedido em Broadcast na rede chamado de DHCP Discover, se houver um servidor DHCP disponível, ele responde com um pacote chamado de DHCP Offer, oferecendo um endereço de IP livre da sua faixa de endereços, esse pacote de resposta é direcionado ao dispositivo que fez o pedido, identificado pelo seu MAC fornecido no DHCP Discover.

2.)

O Teorema de Nyquist pode ser aplicado em qualquer meio físico, pois não depende da natureza do meio mas sim das propriedades matemáticas do sinal transmitido. Desde que o meio físico suporte a largura de banda e as frequências necessárias, o teorema assegura que uma taxa de amostragem superior ao dobro da frequência máxima do sinal original permite a sua reconstrução sem perca de informação.

Assim resumindo o essencial não é o tipo de meio físico, mas a sua capacidade de preservar as características fundamentais do sinal dentro dos limites do teorema em si ou seja desde que o meio físico respeite as condições do teorema (como largura de banda e frequência máxima do sinal) o teorema não dependera do meio físico.

3.)

Não são idênticas pois a rede confiável em fluxo de bytes não preserva a estrutura original da mensagens, exigindo que a aplicação as reconstruia conforme necessário, já a rede que fornece um fluxo de mensagem confiável preserva os limites da estrutura das mensagens originais, entregando-as exatamente como foram enviadas.

Esta diferença afeta a forma como as aplicações interagem com os dados tornando estes dois serviços distintos.

4.)

O CIDR (Class Inter-Domain Routing) é um método de atribuição de endereços de IP que permite a alocação mais eficiente de endereços na Internet. Em vez de usar uma classe fixa de endereços de IP (como Class A, B, ou C), o CIDR permite a atribuição de blocos de endereços de IP de tamanho variável a organizações ou redes utilizado mascaras de sub-rede

variáveis (VLSM - Variable Length Subnet Mask), 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 a escalabilidade do roteamento de pacotes na Internet. O CIDR é utilizado hoje em dia ao lidar com endereços de IPv4 devido a escassez dos mesmos.

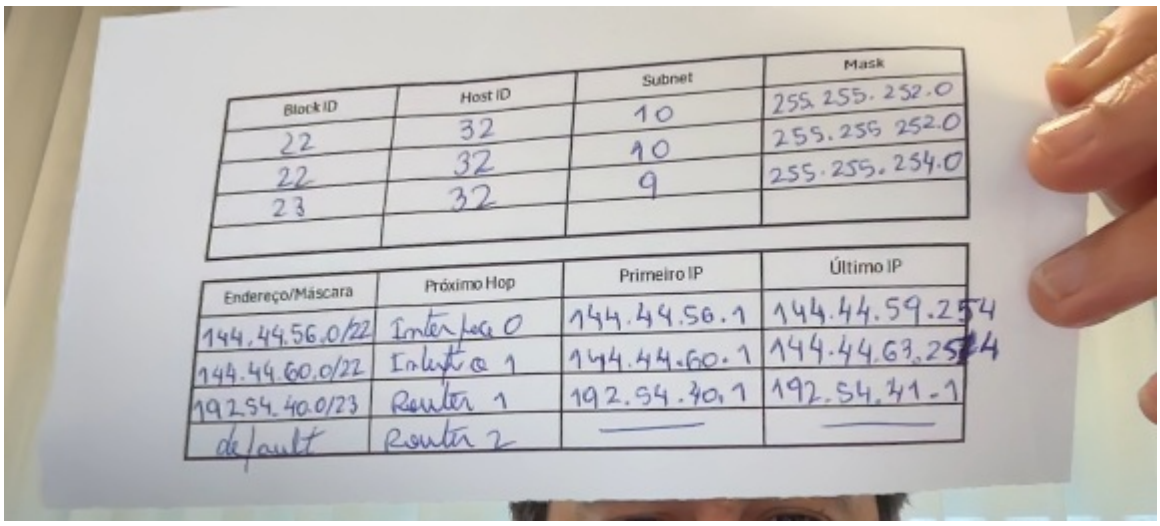
5.)

Embora a maioria dos protocolos modernos como TCP/IP que foi concebidos para minimizar essas situações, adicionando verificações e integridade dos dados e uma entrega correta dos pacotes, sim é possível embora praticamente insignificante em redes bem configuradas e/ou estáveis.

Exemplos disso poderá ser a interferência na comunicação como ruídos eletromagnéticos, falhas em hardware e/ou algum erro nos protocolos de rede.

Resumindo embora improvável de acontecer, sim é possível que um pacote seja entregue no destino errado.

6.)



Block ID	Host ID	Subnet	Mask
22	32	10	255.255.252.0
22	32	10	255.255.252.0
23	32	9	255.255.254.0

Endereço/Máscara	Próximo Hop	Primeiro IP	Último IP
144.44.56.0/22	Interface 0	144.44.56.1	144.44.59.254
144.44.60.0/22	Interface 1	144.44.60.1	144.44.63.254
192.54.40.0/23	Router 1	192.54.40.1	192.54.41.1
default	Router 2	—	—

6.a.)

Para: 144.44.63.10

Como o IP 144.44.63.10 esta dentro do endereço prefixo 144.44.60.0/22 fará hop para o Interface 1.

6.b.)

Para: 192.54.40.7

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

7.a.)

O algoritmo de flooding é usado pelos routers para decidir como encaminhar pacotes na rede. O método consiste em enviar o pacote recebido para todas as conexeçoes de saída, excepto para aquela por onde o pacote chegou. Este algoritmo pode ser aplicado de três formas, flooding não controlado, seletivo e controlado.

Uma vez que flooding pode gerar pacotes duplicados em grande quantidade, a variante controlada utiliza uma técnica para limitar essa mesma propagação, para isso adiciona um contador de hops (saltos) no cabeçalho do pacote, que é reduzido a cada salto que o pacote realiza, quando o contador chega a zero, o pacote é eliminado. O ideal é que este contador seja configurado com um numero de saltos previstos até ao destino, contido se a origem não souber a distancia exata, pode usar um valor que corresponda ao pior cenário, aumentado assim a probabilidade de entrega.

Outra forma de evitar pacotes infinitos, caso o caminho até ao destino já seja conhecido, é a inclusão no cabeçalho um contador TTL (Time To Live), este contador também é decrementado a cada salto e quando atinge zero é removido da rede.

7.b.)

Com o máximo de 4 hops as rotas possíveis são:

A-B-E-G

A-B-D-F-G

A-B-E-F-G

A-C-D-F-G

7.c)

Para calcular o consumo de largura de banda é necessário contabilizar todas as transmissões realizadas. No algoritmo de flooding cada ligação entre routers é apenas realizada 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.

Sendo assim:

A - C uma transmissão

A - B uma transmissão

B - D uma transmissão

B - E uma transmissão

C - D uma transmissão

D - F uma transmissão

E - F uma transmissão

E - G uma transmissão

F - G uma transmissão

Total 9 transmissões

A contagem de 9 hops é o total de ligações percorridas e consequentemente o consumo de largura de banda neste exercício.