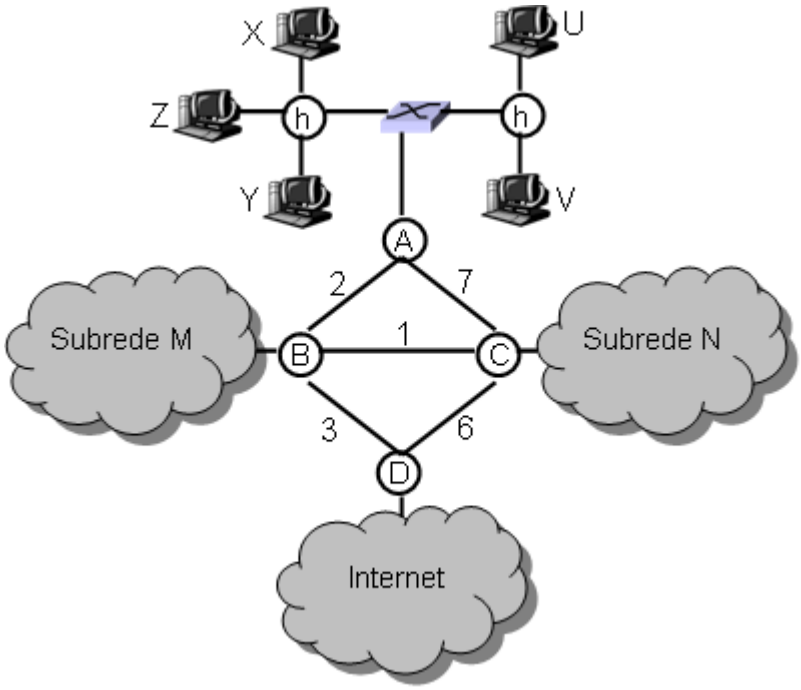
Esse cenário é usado para as questões 1, 2 e 3: Imagine que um computador está se conectando pela primeira vez a uma rede através de uma interface Ethernet. Sem que o usuário saiba, entre ele e seu roteador gateway há um comutador que já conhece o MAC do gateway, mas não do novo computador. Um servidor DHCP está em execução no gateway (o novo computador não tem dados sobre esse servidor, mas o servidor está configurado para responder a mensagens DHCP), de forma que o usuário não precisa configurar sua conexão manualmente. Após conectar-se à rede, o usuário abre seu navegador e digita na barra de endereços o IP 200.144.183.244 de um servidor web.

1 - Para o cenário acima:
a) Descreva passo a passo o que ocorre para que o computador se conecte à rede até poder enviar o primeiro pacote para o servidor em 200.144.183.244. Não esqueça de citar cada passo dos protocolos DHCP e ARP, o auto-aprendizado do comutador, diferenciar endereços IP e MAC e de dizer que mensagens são broadcast, quais são unicast (e para onde) e quais protocolos da camada de transporte (se forem usados), de rede e de enlace são usados pelas mensagens DHCP e ARP. **[1.5]**
b) Explique como o comutador (além de enlaces full-duplex) evita colisões na rede local entre os pacotes do cliente e os de outros hosts da rede. **[0.5]**

2 - O primeiro pacote enviado para o servidor web no cenário acima é para abrir uma conexão TCP.
a) Descreva os passos necessários para que essa conexão seja aberta e para que seja fechada. **[1.0]**
b) Imagine que o servidor esteja operando em modo persistente e que troque um grande número de mensagens com o cliente antes que a conexão seja fechada. Esboce um gráfico de taxa de emissão X tempo mostrando como o controle de congestionamento do TCP atua para sobre a taxa de emissão. Mostre no seu gráfico um evento de três acks duplicados no tempo 1.5s, enquanto ainda ocorria o slow start e a taxa era de 32KB/s, outro no tempo 2s, além de um evento de timeout no tempo 4s (mostre um tempo total de 5s no gráfico). Indique no gráfico quais são os períodos de slow start e congestion avoidance, além de quais trechos tem comportamento linear e quais são exponenciais. **[1.0]**

3 - Para o cenário descrito no começo:
a) Imagine que um dos pacotes enviados do servidor para o cliente tenha ID 123, tamanho total de 1400 bytes, um cabeçalho IPv4 com o tamanho padrão de 20 bytes e que chegue completo no gateway, mas que o MTU do enlace entre o gateway e o cliente seja somente de 820 bytes. Mostre como o pacote é fragmentado indicando o tamanho, a ID, a fragflag e o deslocamento dos pacotes resultantes. **[1.0]**
b) Explique como é calculado um CRC de r bits na camada de enlace para os pacotes entre o cliente e o gateway. Quantos erros esse CRC permite detectar? Ele permite a correção desses erros? Se sim, explique como e se não cite um exemplo de outro algoritmo que permita a correção de erros. **[1.0]**

4 - Na figura ao lado: A, B, C e D são roteadores; U, V, X, Y e Z são hosts, dois hubs estão indicados com h e X é um comutador.
a) O administrador da rede tem os endereços 200.144.183/24 para distribuir entre UVXYZ e as subredes M e N. A subrede M deve suportar 60 interfaces e a N deve suportar 80. Dê endereços e máscaras de subrede para os hosts e para as subredes. **[1.0]**
b) Com os custos dos enlaces dados na figura, mostre como funciona o algoritmo de roteamento usado no OSPF para rotas de C para os outros roteadores. **[1.0]**



Para fazer em casa sobre segurança (entregar respostas impressas e folha de questões em sala em 26/11!):

1) Explique o que são os aspectos de confidencialidade, autenticação, integridade da mensagem e disponibilidade de serviços e como estão relacionados à segurança de redes. Dê ao menos um exemplo prático para cada um desses aspectos em que garantir sua segurança é importante e dê ao menos um exemplo de ataque que busca violar essa segurança.

2) O que são chaves criptográficas? Explique como funciona a criptografia de chave simétrica e a criptografia de chave pública.

3) Explique como funciona Cypher Block Chaining. Contraste a criptografia de bloco (como CBC) com a criptografia de fluxo (como na RC4 usado em WEP).

4) Mostre como gerar um par de chaves usando RSA e os números primos 11 e 17. Mostre como essas chaves seriam usadas para codificar e depois para decodificar o caracter ASCII (8 bits) da primeira letra (maiúscula) de seu nome.

5) Explique como as chaves pública e privada podem ser usadas "de forma invertida" para assinar digitalmente uma mensagem e para conferir a assinatura.

6) Explique como funções de HASH podem ser usadas para autenticar o remetente e garantir a integridade da mensagem sem criptografia.

7) Explique o que é um nonce, o que é um ataque de reprodução e como o primeiro evita o segundo.

8) Explique como funciona SSL.