Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 - GABARITO - 2° semestre de 2008

1ª questão (1.5 pontos)

Considere o tipo de serviço oferecido pela Internet de hoje, conhecido como *best effort*. Responda às perguntas abaixo.

1. (0.5 ponto) Por que este tipo de serviço, de forma geral, não é adequado para aplicativos multimídia?

   Resposta:

   Porque o serviço *best effort* não oferece nenhum tipo de garantia com relação a taxa de transmissão de pacotes nem com relação ao atraso fim-a-fim dos pacotes. Como aplicativos multimídia são muito sensíveis ao atraso e a variações no atraso, este serviço não é adequado.

2. (0.5 ponto) Cite duas técnicas empregadas por aplicativos multimídia para mascarar os efeitos negativos do serviço *best effort*. Para cada técnica citada, descreva quais efeitos negativos estão sendo mascarados pela técnica.

   Resposta:

   Bufferização do lado do cliente. O objetivo desta técnica é mascarar os atrasos impostos pela rede aos pacotes dos aplicativos. Mais ainda, esta técnica serve para mascarar as variações do atraso dos pacotes, pois pequenas variações são aliviadas pelo buffer do lado do cliente.

   Protocolo UDP. Ao utilizar o protocolo de transmissão UDP, os aplicativos multimídia não estão sujeitos a variação da taxa de transmissão imposta pelo protocolo TCP, que adapta a taxa de transmissão devido ao mecanismo de controle de congestionamento. Ao utilizar o protoclo UDP, os aplicativos estarão menos sujeitos a variações na taxa de transmissão.

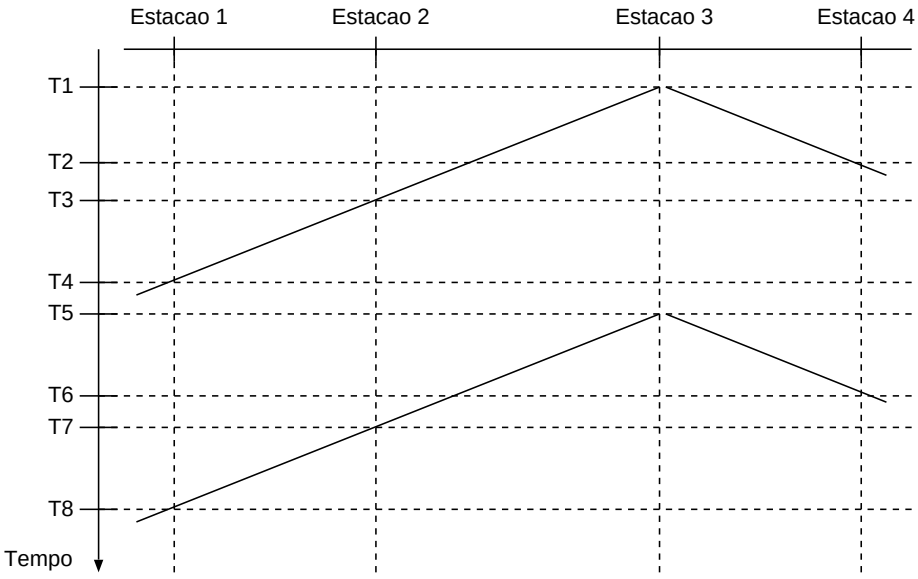
3. (0.5 ponto) Descreva como funciona o mecanismo de bufferização do lado do cliente.

   Resposta:

   A bufferização do lado do cliente consiste em utilizar um buffer no programa do cliente para armazenar temporariamente os pacotes pertinentes ao fluxo multimídia sendo enviado pelo servidor. Ao invés de iniciar a decodificação e apresentação do conteúdo imediatamente, o cliente aguarda a chegada de alguns pacotes armazenando-os em um buffer local. Após a chegada de um determinado número de pacotes, o cliente inicia a decodificação e a apresentação do contúdo. Este procedimento leva a um atraso inicial na decodificação e apresentação do conteúdo, mas torna o aplicativo mais tolerável a variações do atraso de pacotes pela rede.

2ª questão (2.0 pontos)

1. (0.5 pontos) Considere o protocolo de acesso aleatório CSMA. Explique porque colisões podem ocorrer e como funciona o protocolo quando uma colisão ocorre.



2. (1.5 pontos) Considere o exemplo ilustrado na figura abaixo, onde 4 estações utilizam o protocolo CSMA para compartilhar o meio. Considerando a linha de tempo ilustrada na figura e o fato de que a estação 3 inicia uma transmissão no instante de tempo $T1$, responda às perguntas abaixo.

   (a) (0.5 pontos) Em que instantes de tempo as estações 1, 2 e 4 terminam de receber a transmissão da estação 3?

   Resposta: Estação 1 em T8, estação 2 em T7, e a estação 4 em T6.

   (b) (0.5 pontos) Explique porque a estação 2 começa a receber a transmissão da estação 3 depois da estação 4.

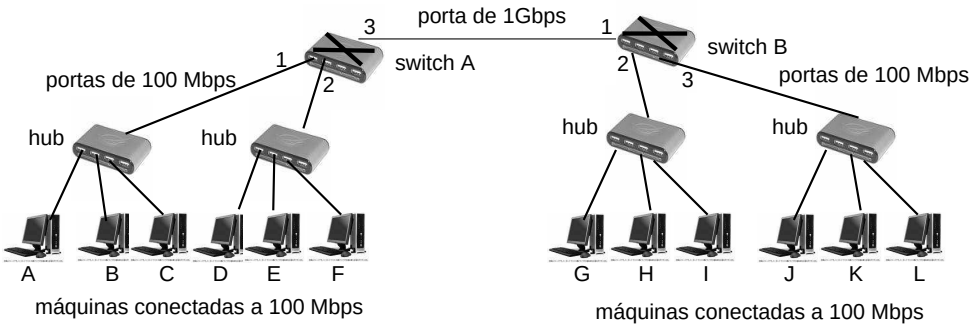
   Resposta: Porque o sinal de transmissão enviado pela estação 3 demora mais para se propagar até a estação 2 do que para se propagar até a estação 4. Possivelmente, a estação 2 está mais longe fisicamente da estação 3 do que a estação 4, lembrando que o tempo de propagação do sinal é proporcional a distância física.

   (c) (0.5 pontos) Em que instantes de tempo (indique todos, se for o caso) a estação 2 está livre para iniciar uma transmissão? Explique sua resposta.

   Resposta: A estação 2 pode iniciar uma transmissão em qualquer instante antes de T2 e qualquer instante após T7. Nestes instantes, ao escutar o meio, a estação 2 não irá detectar uma transmissão em andamento e poderá então iniciar sua transmissão.

3ª questão (2.5 pontos)

Considere na rede abaixo que o *host B* envia uma mensagem para *o host K* e, em seguida, *K* responde à mensagem de *B*. Suponha que a tabela de encaminhamento do switch A e a tabela do switch B estejam fazias no momento do envio da primeira mensagem. Considere também que todas as portas dos hubs e switches sejam de 100 Mbps, exceto a porta que liga os dois switches.



1. (0.5) Por qual(is) interface(s) de saída do switch A e do switch B a mensagem do *host B* destinada ao *host K* será encaminhada ? (Explique porquê.)

   Resposta:

   No switch A será encaminhada pelas interfaces 2 e 3. Como a tabela de encaminhamento do switch A está vazia, o algoritmo usado é o *flooding*.

   No switch B será encaminhanda pelas interfaces 2 e 3. Da mesma forma que para o switch A, como a tabela de encaminhamento do switch B está vazia, o algoritmo usado é o *flooding*.

2. (0.5) Por qual(is) interface(s) de saída do switch A e do switch B a mensagem do *host K* destinada ao *host B* será encaminhada ? (Explique porquê.)

   Resposta:

   No switch B, será encaminhada pela interface 1. No momento que a mensagem do *host B* chegou ao switch B, houve uma atualição na sua tabela e foi criada uma entrada que relaciona o *host B* com a interface 1.

   No switch A, será encaminhada pela interface 1. No momento que a mensagem do *host B* chegou ao switch A, houve uma atualição na sua tabela e foi criada uma entrada que relaciona o *host B* com a interface 1.

3. (0.5) Construa as tabelas de roteamento dos switch A e B após a troca das duas mensagens entre *B* e *K*.

   Resposta:

   Tabela do switch A:

endereço	Interface
B	1
K	3

   Tabela do switch B:

endereço	Interface
B	1
K	3

4. (0.5) Suponha que todas as máquinas estejam ligadas e gerando dados na rede. Qual a vazão (dados gerados pelas máquinas por unidade de tempo) máxima no canal que liga os switches (canal switch A/porta 3 - switch B/porta 1) ?

   Resposta:

   A vazão é de 400 Mbps (200 em cada sentido do canal).

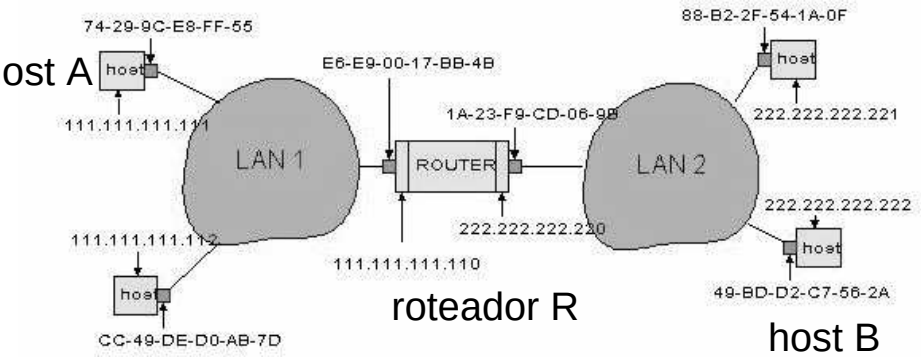
5. (0.5) Se você quizesse aumentar a vazão da rede da figura acima, o que você faria ?

   Resposta:

   Substituiria os *hubs* por switches. Cada switch substituindo um *hub*, teria 3 portas de 100Mbps para ligar os *hosts* e uma porta Giga para se conectar com o switch A/B. Desta forma a vazão máxima alcançada entre os switches A e B seria de 1Gbps.

4ª questão (1.0 ponto)

Considere na rede da figura abaixo que o *host A* quer enviar uma mensagem para o *host B*. Suponha que a tabela ARP de *A* esteja vazia. Descreva as mensagens trocadas na rede (pelo protocolo ARP) até que *A* possua as informações necessárias para enviar a mensagem para *B*.



Resposta:

Passo 1: A envia pacote ARP query em broadcast contendo endereço IP do roteador pois descobre através da sua tabela de roteamento IP que B não está na mesma rede local que ele, portanto deve encaminhar a mensagem para o roteador.

Passo 2: O roteador recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de A.

Passo 3: A recebe o pacote do roteador e atualiza a sua tabela ARP criando uma entrada com o endereço IP do roteador e o respectivo MAC. A envia quadro cujo endereco MAC de destino é o MAC do roteador. Neste quadro, A encapsula o pacote destinado a B (IP destino é B).

Passo 4: Quando o roteador receber o quadro enviado por A, ele usará o IP destino de B para descobrir por qual interface deve encaminhá-lo.

5ª questão (1.0 ponto)

Dê exemplo de duas técnicas para compartilhar o meio de transmissão usadas em redes celulares e explique resumidamente como funcionam.

Resposta:

Combinação de FDMA/TDMA: Divisão do espectro em faixas de frequência e cada faixa de frequência é dividida em slots de tempo. Para cada terminal é alocada uma faixa de frequência e um slot de tempo.

CDMA: Multiplexação por divisão de código. Todos os terminais transmitem ao mesmo tempo, cada um usando um determinado código.

$6^{\underline{a}}$ questão (2.0 pontos)

Segurança em Redes: Responda às perguntas abaixo.

1. (0.5 ponto) De forma geral, o *message digest* de uma mensagem M nada mais é do que um resumo de M. Como podemos obter este resumo? Para que serve este resumo?

   Resposta: O message digest pode ser obtido através de uma função hash, ou seja, através de uma manipulação algébrica determinística da mensagem original que produza um resumo de tamanho fixo. Um exemplo é a função hash criptográfica MD5, que produz um message digest de 128 bits. Existem muitas funcionalidades para um message digest, mas uma das mais importantes serve para verificar a integridade da mensagem. Ou seja, o transmissor envia juntamente com a mensagem M o seu message digest $H(M)$. O receptor então verifica se a mensagem recebida M' possui o digest recebido $H(M)$. Desta forma, um erro na mensagem será detectado pelo receptor, pois o digest de M' não será igual a $H(M)$ que foi recebido.

2. (0.5 ponto) Que problema de segurança é causado por *IP Spoofing*? Descreva uma maneira simples para evitar este problema.

   Resposta: *IP Spoofing* acontece quando um computador na Internet transmite um pacote com endereço IP de origem arbitrário, que não é o endereço IP vinculado ao computador. Uma maneira de evitar este tipo de problema é utilizar filtros de saída nos gateways das redes locais ou nos roteadores. De posse destes filtros, os gateways ou roteadores não encaminham pacotes cujo endereço IP de origem não seja apropriado (por exemplo, não encaminhar pacotes cujo endereço IP de origem não pertença a rede local).

3. (1.0 ponto) Considere que Ana deseja enviar uma mensagem M para Bruno. Bruno gostaria de ter certeza de que a mensagem foi realmente escrita por Ana, e não é forjada. Utilizando primitivas criptográficas de chave pública/privada, descreva os passos necessários para garantir esta propriedade na comunicação entre Ana e Bruno.

   Resposta: Para garantir que a mensagem M foi realmente escrita por Ana, Bruno poderia pediar a Ana para assinar criptograficamente a mensagem M e enviar a assinatura juntamente com M. Para fazer isto, Ana deve utilizar sua chave privada, que é apenas de seu conhecimento, e codificar M, dando origem a $K_A^-(M)$. Isto é a assinatura criptográfica de Ana para da mensagem M. Ao receber M e $K_A^-(M)$, Bruno verificar se Ana realmente escreveu M utilizando a chave pública de Ana K_A^+, que é de conhecimento de todos. Bruno aplica a chave pública de Ana à assinatura recebida, ou seja, $K_A^+(K_A^-(M))$ e verifica se o resultado deste procedimento é igual a mensagem M recebida. Caso positivo, então Ana realmente assinou M, pois $K_A^+(K_A^-(M)) = M$.