# Curso de Tecnologia em Sistemas de Computação
# Disciplina: Redes de Computadores II
# AP2 - 2° semestre de 2007

## 1ª questão (2.5 pontos)

**Aplicações Multimídia**: Responda às perguntas abaixo.

1. (0.5 ponto) Sabemos que *jitter* é a variação do retardo entre os diferentes pacotes de um mesmo fluxo. Explique porque o retardo é variável. É possível ter retardo sem variação em uma rede qualquer?

   **Resposta:**

   O retardo dos pacotes de um mesmo fluxo é variável pois as condições da rede variam no tempo. Mais especificamente, o tamanho das filas dos roteadores variam. Desta forma, um pacote pode encontrar filas menores e um outro do mesmo fluxo filas maiores, tendo retardos bem diferentes.

   Sim, é possível ter retardo sem variação. Imagine o caso onde todas as filas dos roteadores estão sempre vazias. Desta forma, todos os pacotes de um mesmo fluxo terão o mesmo retardo, que será dado pelo retardo de propagação, pelos retardos de transmissão e pelos retardos de processamento (que são praticamente constantes). Este cenário ocorre em redes comutadas por circuito.

2. (0.5 ponto) Por que é mais difícil melhorar a qualidade de aplicativos interativos de áudio em tempo real do que aplicativos streaming de áudio armazenado?

   **Resposta:**

   Porque para manter a boa interatividade os requerimentos de tempo são muito mais estritos. Ou seja, em aplicativos streaming de áudio armazanado, o cliente pode esperar alguns segundos antes do conteúdo ser iniciado sem maiores problemas. Isto permite ao aplicativo maior flexibilidade, por exemplo, aumentando o tamanho do buffer de playout. Entretanto, em aplicativos interativos de áudio, para manter a boa interatividade, o aplicativo não poder esperar tanto tempo, tendo muito menos flexibilidade.

3. (1.5 ponto) Aplicativos multimídia na Internet tendem a utilizar uma série de técnicas para lidar com o serviço "best effort"e melhorar o desempenho da aplicação. Cite três destas técnicas e descreva como cada uma delas ajuda os aplicativos.

   **Resposta:**

   - **Bufferização do lado do cliente.** A técnica consiste em criar um buffer do lado do cliente onde os pacotes são armazenados antes de serem decodificados. O aplicativo do lado do cliente aguarda um tempo entre a chegada do primeiro pacote do fluxo até o início da decodificação e apresentação do conteúdo para o cliente. O objetivo é reduzir o jitter introduzido pela rede.

- **Protocolo de transporte.** A técnica consiste em utilizar o protocolo UDP ao invés do tradicional protocolo TCP. O protocolo UDP não possui controle de congestionamento nem oferece uma transmissão confiável e por isto permite ao servidor a enviar os dados a taxa apropriada (taxa de codificação). O objetivo é fazer com que os pacotes cheguem mais rapidamente ao cliente, e possivelmente reduzindo o jitter.
- **Múltipla codificação da mídia.** A técnica consiste em codificar o conteúdo com taxas diferentes, armazenando estas diferentes codificações no servidor. O objetivo é melhor casar a taxa de acesso do cliente com a taxa de codificação do conteúdo. Destar forma, clientes com maior banda passante podem assitir a um conteúdo com melhor qualidade, sem prejudicar clientes que possuem banda passante menores.

## 2ª questão (2.5 pontos)

**Segurança em Redes**: Responda às perguntas abaixo.

1. (0.5 ponto) Explique porque criptografia com chave simétrica é fundamentalmente diferente de criptografia com chave pública/privada.

   **Resposta:**

   A diferença fundamental está nas chaves. Na criptografia com chave simétrica as duas partes comunicantes precisam compartilhar o mesmo segredo, que é a chave simétrica. Na criptografia com chave pública/privada, a chave utilizada para cifrar os dados é pública, ou seja, é de conhecimento de todos. A chave privada é de conhecimento apenas da parte que irá receber a mensagem cifrada e serve para decifrar a mensagem. Desta forma, as duas partes comunicantes não precisam compartilhar um segredo.

2. (0.5 ponto) Considere um firewall que permite que os computadores que estejam dentro da rede protegida acessem a Web. Ou seja, o firewall possui uma regra que encaminha corretamente pacotes do protocolo TCP com porta 80. Considere agora um outro aplicativo qualquer (ex. Kazaa) que utiliza o mesmo protocolo e porta. Os pacotes gerados por tal aplicativo serão encaminhados pelo firewall? Explique sucintamente sua resposta.

   **Resposta:**

   Sim, os pacotes do tal aplicativo serão encaminhados corretamente pelo firewall. Isto ocorre pois o firewall filtra os pacotes individualmente, seguindo rigorasamente as regras que foram estabelecidas, independente do aplicativo que esteja gerando os pacotes. Assim sendo, se um pacote está dentro das regras estabelecidas, o mesmo será encaminhado pelo firewall.

3. (1.5 ponto) Suponha que Ana quer enviar uma mensagem $M$ à Bruno. Ela deseja que somente Bruno tenha acesso ao conteúdo da mensagem e que ele também tenha certeza de que foi ela quem redigiu a mesma. Utilizando criptografia com chaves públicas/privadas e assumindo que ambos possuem a chave pública do outro, *(i)* descreva os passos que Ana deve realizar para enviar tal mensagem; *(ii)* descreva o que Bruno precisa fazer para ler a mensagem.

   **Resposta:**

   Passos que Ana precisa realizar:

- Ana deve utilizar a chave pública de Bruno para cifrar a mensagem $m$, gerando $K_B^+(m)$. Isto garante que apenas Bruno, através de sua chave privada, poderá ler a mensagem.
- Ana deve utilizar sua chave privada para cifrar a mensagem $m$, gerando $K_A^-(m)$. O resultado é a assinatura de Ana, o que irá permitir a Bruno verificar que Ana redigiu a mesagem.
- Ana deve utilizar a chave pública de Bruno para cifrar sua assinatura, gerando $K_B^+(K_A^-(m))$. Isto é necessário, pois caso contrário um intruso poderia utilizar a chave pública de Ana para ler a mensagem!
- Ana deve enviar a Bruno a mensagem e a assinatura cifrada.

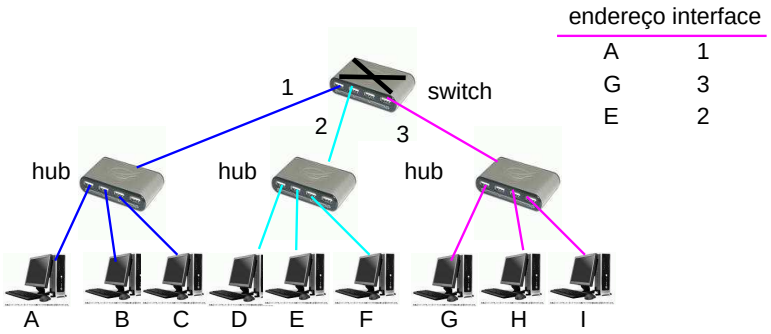
Passos que Bruno precisa realizar:

- Bruno decifra $K_B^+(m)$ utilizando sua chave privada e recupera a mensagem $m$.
- Bruno decifra $K_B^+(K_A^-(m))$ utilizando sua chave privada e recupera a assinatura de Ana, ou seja, $K_A^-(m)$.
- Utilizando a chave pública de Ana, Bruno decifra a assinatura $K_A^-(m)$ e compara o resultado com a mensagem $m$, decifrada no primeiro passo. Se as duas mensagens são iguais, então Ana redigiu $m$.

## 3ª questão (2.5 pontos)

**Interconexão de redes**

Considere na rede abaixo que o *host B* envia uma mensagem para *o host F* e, em seguida, *F* responde à mensagem de *B*. Os hosts *B* e *F* estão interconectados através de um switch que possui a tabela de encaminhamento mostrada na figura abaixo.




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

   **Resposta:**

   Será encaminhada pela interface 1 pois o switch possui uma entrada na sua tabela para o host B. Esta entrada foi inserida na tabela quando o host B enviou uma mensagem para F.

2. (0.5) Construa a tabela de roteamento do switch após a troca de mensagens entre *B* e *F*.

   **Resposta:**

| endereço | interface |
|---|---|
| A | 1 |
| G | 3 |
| E | 2 |
| B | 1 |
| F | 2 |

3. (0.5) Se ao invés de um switch, o equipamento usado para interconexão fosse um hub, por qual(is) interface(s) a mensagem de $B$ para $F$ seria encaminhada ? (Explique porquê.)

   **Resposta:**

   Seria encaminhada pelas interfaces 2 e 3 pois o hub é um simples repetidor: encaminha a mensagem por todas as interfaces de saída, exceto àquela pela qual recebeu a mensagem.

4. (0.5) Descreva um cenário em que pode ocorrer troca de mensagens entre hosts quaisquer e o switch não encaminhá-las por nenhuma de suas interfaces.

   **Resposta:**

   Esta situação ocorre quando um *host* envia uma mensagem para outro *host* que está no mesmo segmento de LAN, por exemplo, em uma troca de mensagens entre A e B.

5. (0.5) Cite duas características que diferenciam os switches de roteadores.

   **Resposta:**

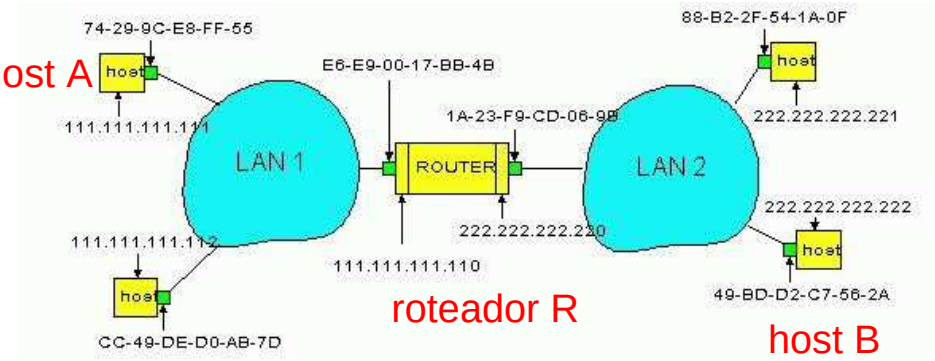
   1 - Switches não implementam algoritmo para cálculo do melhor caminho de uma origem até um certo destino na rede. As tabelas de encaminhamento são geradas através de um algoritmo de aprendizado.

   2 - Switches não necessitam de intervenção de um administrador para entrarem em operação, são *plug and play*, diferentemente dos roteadores que necessitam ser configurados por um administrador.

## 4ª questão (1.0 ponto)

**Protocolo ARP**

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.

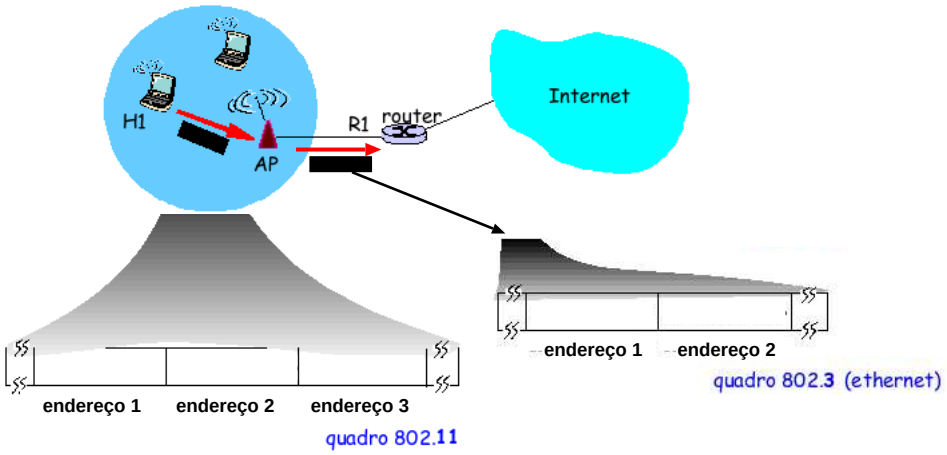
Passo 3: A recebe o pacote do roteador e atualiza a sua tabela ARP criando uma entrada com o endereço IP do roteador e o respectivo MAC. A envia quadro cujo endereco MAC de destino é o MAC do roteador. Neste quadro, A encapsula o pacote destinado a B (IP destino é B).

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 (1.5 pontos)

**Redes sem fio**

Considere a topologia da figura abaixo, onde um *host H1* está enviando uma mensagem que deve ser roteada pelo roteador *R1*. *H1* está em uma rede IEEE802.11 infra-estruturada e o AP (ponto de acesso) desta rede, está ligado a Internet através do roteador *R1*.




1. (0.5) Descreva quais endereços devem estar contidos nos campos *endereço 1,2 e 3* do quadro 802.11 e nos campos *endereço 1 e 2* do quadro ethernet. (Por exemplo, endereço MAC do AP.)

   **Resposta:**

   Quadro 802.11:

   Endereço 1: endereco MAC do AP (estacão de destino).

   Endereço 2: endereco MAC de H1 (estacão de origem).

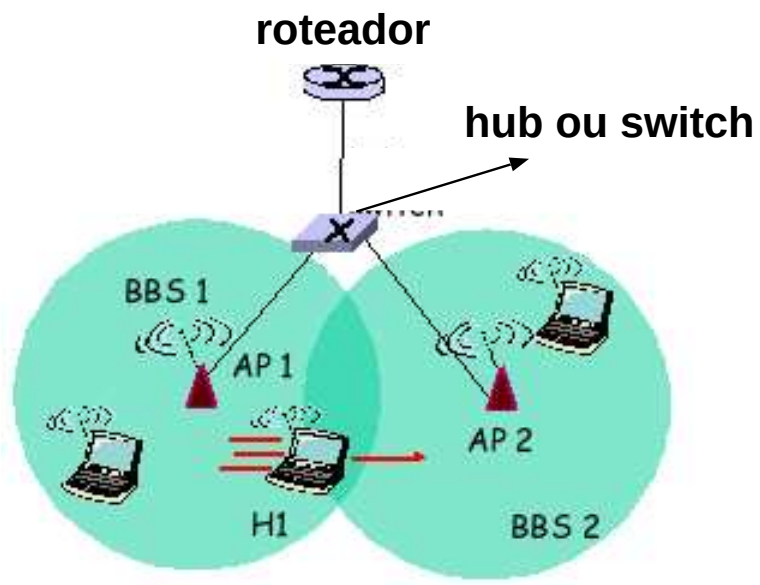
   Endereço 3: endereco MAC do roteador que está conectando a sub-rede da BSS a outras sub-redes. Na figura acima é o endereco MAC do roteador R1.

   Quadro ethernet:

   Endereço 1: endereco MAC de R1 (estacão de destino).

   Endereço 2: endereco MAC de H1 (estacão de origem).

2. Suponha que o host *H1* se desloque e passe a ser atendido por um outro AP conforme a figura abaixo.




3. (0.5) Considerando que a interconexão é feita usando um hub, o deslocamento de *H1* interfere no funcionamento do hub ? (Explique porquê).

   **Resposta:**

   Não, pois o hub não possui tabela de encaminhamento e portanto não faz encaminhamento seletivo dos quadros para as sub-redes adequadas.

4. (0.5) No caso da interconexão ser feita com um switch, descreva um cenário em que pacotes de uma conexão de *H1* podem ser perdidos devido ao seu deslocamento.

   **Resposta:**

   Suponha que *H1* se desloque para a BSS2 e a tabela de encaminhamento do switch ainda não tenha sido atualizada pois *H1* ainda não transmitiu nenhuma mensagem desde que chegou na BSS2. Neste caso, até que *H1* envie uma mensagem e a tabela do switch seja atualizada, todas as mensagens destinadas a *H1* serão perdidas.