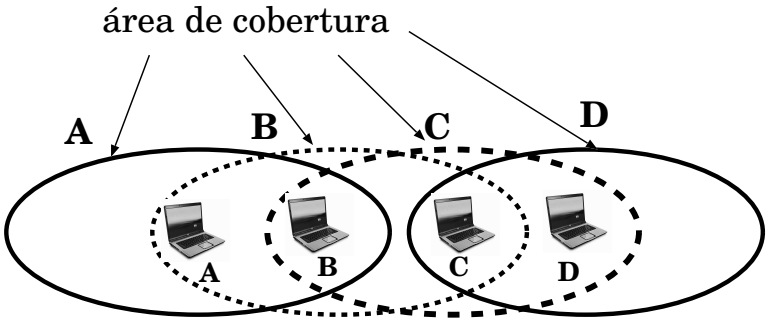
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 1° semestre de 2010

1ª questão (3.0 pontos)

Redes sem fio



Considere o cenário da figura acima onde existem 4 terminais móveis, A, B, C e D, operando o protocolo IEEE 802.11 no modo *ad hoc*. A área de cobertura de cada um deles é mostrada através das elipses na figura. Suponha que todos os nós compartilham a mesma frequência. A transmissão de A só é recebida por B; quando B transmite, ambos A e C recebem o sinal; a transmissão de C é recebida por B e D; e quando D transmite, somente C pode ouví-lo.

Suponha que cada nó tem um número muito grande de mensagens para enviar. Caso a mensagem não seja endereçada para um vizinho, ela deve ser re-encaminhada pelo vizinho. Por exemplo, se A quer enviar uma mensagem para D, a mensagem passará por B e C até chegar a D.

O tempo é dividido em slots e a transmissão de uma mensagem leva exatamente um slot de tempo. Durante um slot um terminal pode: (i) enviar uma mensagem, (ii) receber uma mensagem (se somente uma mensagem está sendo enviada) e (iii) ficar em silêncio. Se um nó escuta duas ou mais transmissões simultaneas, ocorre uma colisão e nenhuma das mensagens são recebidas com sucesso.

1. Suponha que em um slot de tempo somente A e C tenham mensagens para enviar para B.

   (a) (0.5) Neste cenário, ocorrerá uma colisão ? Explique porquê.

   Resposta:

   Sim, pois B está na área de cobertura de A e C e portanto receberá a mensagem de ambos A e C ao mesmo tempo.

(b) (0.5) A mensagem enviada de C para B pode ser *ouvida* pelo terminal A ? Por quê ?

Resposta:

Não, pois A não está na área de cobertura de C.

2. Considere agora que em um slot de tempo, A tem uma mensagem para enviar para B e D tem uma mensagem para enviar para C.

   (a) (0.5) Neste caso, vai ocorrer uma colisão ? Explique porquê.

   Resposta:

   Não, pois B não está na área de cobertura de D (está na área de A que enviou a mensagem para ele) e C não está na área de cobertura de A (está na área de D que enviou a mensagem para ele).

   (b) (0.5) Qual a vazão máxima em *mensagens/slot de tempo* alcançada por A e por D ?

   Resposta:

   A vazão máxima é de uma mensagem por slot de tempo.

   (c) (0.5) Se a mensagem fosse enviada de C para D ao invés de D para C, ocorreria uma colisão ? Explique porquê.

   Resposta:

   Sim, pois neste caso B receberia tanto a mensagem enviada por A quanto a mensagem enviada por C pois está na área de cobertura de ambos.

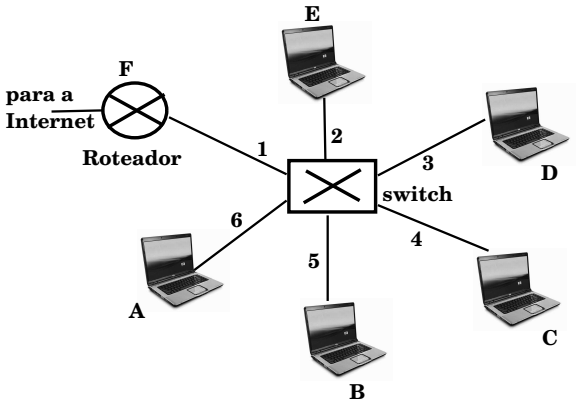
3. (0.5) Suponha que A envie uma mensagem destinada a D, e que nenhum outro terminal vá transmitir mensagens até que a mensagem chegue em D. Qual a vazão máxima em *mensagens/slot de tempo* que pode ser alcançada nesta transmissão de uma mensagem de A para D ?

   Resposta:

   A vazão máxima é de uma mensagem a cada 3 slots de tempo.

2^{a} questão (3.0 pontos)

Interconexão de redes



Considere o cenário da figura acima onde um switch interconecta diversos computadores e um roteador. Suponha que inicialmente a tabela do switch está vazia. Considere que as mensagens abaixo são enviadas. Mostre o estado da tabela do switch após o recebimento de cada uma delas e por quais interfaces do switch cada uma das mensagens deve ser encaminhada. Justifique suas respostas.

1. (0.5) B envia uma mensagem para E.

   Resposta:

endereço	Interface
B	5

   A mensagem será encaminhada por todas as interfaces exceto a interface 5.

2. (0.5) E envia uma resposta para B.

   Resposta:

endereço	Interface
B	5
E	2

   A mensagem será encaminhada pela interface 5.

3. (0.5) C envia uma mensagem para B.

   Resposta:

   A mensagem será encaminhada pela interface 5.

4. (0.5) B envia uma resposta para C.

   Resposta:

   A mensagem será encaminhada pela interface 4.

Suponha que todos os links que interconectam os computadores com o switch são de 100 Mbps e que o link que interconecta o switch com o roteador é de 1 Gbps.

endereço	Interface
B	5
E	2
C	4

endereço	Interface
B	5
E	2
C	4

1. (0.5) Considere que todos os computadores estão transmitindo dados para serem encaminhados pelo roteador para a Internet. Qual a vazão máxima entre esta rede e a Internet ?

   Resposta:

   A vazão máxima é de 500Mbps.

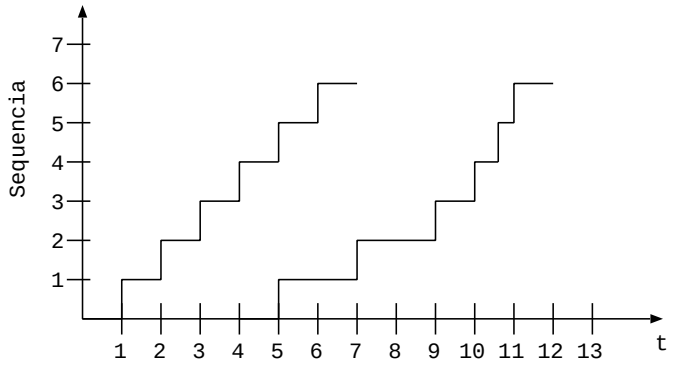
2. (0.5) No cenário acima, se ao invés de um switch, o equipamento fosse um hub com portas de 100Mbps, qual seria a vazão máxima entre esta rede e a Internet ?

   Resposta:

   A vazão méxima seria de 100Mbps.

$3^{\underline{a}}$ questão (2.0 pontos)

Aplicações multimídia. Considere o gráfico abaixo que ilustra os instantes da transmissão e recebimento de pacotes de uma aplicação multimídia (ex. pacotes de áudio).



1. (0.5) Determine os instantes de transmissão e de recebimento de cada um dos pacotes.

   Resposta: Os instantes de transmissão e recebimento estão assinalados nas duas curvas apresentadas no gráfico. Seja T_i e R_i os instantes de transmissão e recebimento do pacote i, com $i = 1, 2, \ldots$. Assim sendo, temos: $T_1 = 1$, $R_1 = 5$, $T_2 = 2$, $R_2 = 7$, $T_3 = 3$, $R_3 = 9$, $T_4 = 4$, $R_4 = 10$, $T_5 = 5$, $R_5 = 10.5$, $T_6 = 6$, $R_6 = 11$.

2. (0.5) Determine o atraso sofrido por cada um dos pacotes.

   Resposta: O atraso sofrido por um pacote é dado pelo seu tempo de recebimento menos seu tempo de transmissão, ou seja, $R_i - T_i$. Seja $A_i = R_i - T_i$ o atraso sofrido

pelo pacote i, com $i = 1, 2, \ldots$. Assim sendo, temos que: $A_1 = 4$, $A_2 = 5$, $A_3 = 6$, $A_4 = 6$, $A_5 = 5.5$, $A_6 = 5$.

3. (0.5) Assuma que a decodificação dos pacotes pelo cliente irá iniciar no instante de recebimento do primeiro pacote. Quais pacotes serão perdidos por não ainda não terem chegado no cliente no instante em que deveriam ser decodificados?

   Resposta: Se a decodificação iniciar no instante de recebimento do primeiro pacote, todos os pacotes com atraso maiores do que o atraso do primeiro pacote serão perdidos. Isto ocorre pois o a decodificação precisa ser feita a uma taxa constatante, idêntica a taxa de codificação dos pacotes. No exemplo acima, o pacote 1 possui um atraso $A_1 = 4$, e assim sendo, todos os outros pacotes serão perdidos, pois todos os outros possuem um atraso maior do que 4.

4. (0.5) Assuma agora que a decodificação dos pacotes pelo cliente irá iniciar **duas unidades de tempo depois** do instante de recebimento do primeiro pacote. Quais pacotes serão perdidos por não ainda não terem chegado no cliente no instante em que deveriam ser decodificados?

   Resposta: Se a decodificação irá começar duas unidades de tempo depois, então todos os pacotes que possuem um atraso maiores do que $A_1 + 2$ serão perdidos. No caso, como $A_1 = 4$, temos que todos os pacotes que soferem um atraso maior que 6 serão perdidos. No exemplo acima, nenhum pacote possui atraso maior do que seis, logo nenhum pacote será perdido.

$4^{\underline{a}}$ questão (2.0 pontos)

Segurança em redes. Responda às perguntas abaixo.

1. (1.0) Sejam K_A^+ e K_A^- as chaves públicas e privadas de Ana, respectivamente. Sejam K_B^+ e K_B^- as chaves públicas e privadas de Bruno, respectivamente. Seja m uma mensagem em texto que Ana deseja enviar a Bruno com confidencialidade. Indique se cada afirmação é verdadeira ou falsa.

   (a) Ana deve informar K_A^- a Bruno antes de transmitir m.
   Resposta: Falso. K_A^- é a chave privada de Ana e nunca deve ser informada a outra pessoa, pois somente Ana deve conhecer esta chave.

   (b) Bruno deve informar K_B^+ a Ana antes dela transmitir m.
   Resposta: Verdadeiro. Para Ana cifrar a mensagem m ela precisa conhecer a chave pública de Bruno, ou seja, de K_B^+.

   (c) $K_A^+(m) = K_B^-(m)$.
   Resposta: Falso. A chave pública de Ana (K_A^+) não tem nenhuma relação com a chave privada de Bruno(K_B^-).

   (d) $K_B^+(m) = K_B^-(m)$.
   Resposta: Falso. A chave públiva de Bruno aplicada a uma mensagem m não produz o mesmo texto cifrado que a chave privada de Bruno aplicada a mesma mensagem m.

   (e) Bruno não precisa conhecer nenhuma chave de Ana para receber m com confidencialidade.
   Resposta: Verdadeiro. Ana envia a Bruno $K_B^+(m)$ que é a mensagem m cifrada com a chave pública de Bruno. Ao receber a mensagem, Bruno aplica sua chave

privada ao texto cifrado obtendo m, ou seja, $K_B^-(K_B^+(m)) = m$. Assim sendo, Bruno não precisa conhecer nenhuma chave de Ana para receber m com confidencialidade.

2. (1.0) Descreva como *message digests* podem ser utilizados para garantir a integridade da comunicação. Em particular, descreva os passos que tanto o transmissor quanto o receptor devem realizar para garantir a integridade de uma mensagem m.

   Resposta: O *message digest* é gerado a partir de uma função de hash criptográfica, como por exemplo, a função de hash MD5 ou SHA-1. Seja, h uma função de hash criptográfica utilizada para gerar o *message digest*. Assim sendo, dado uma mensagem m, o seu message digest é dado por $h(m)$. Para garantir a integridade de uma mensagem m, o transmissor deve calcular o message digest $h(m)$ e transmitir as duas partes, ou seja, $\{m, h(m)\}$. O receptor, ao receber as duas partes, calcula o message digest da mensagem recebida. Seja, m' a mensagem recebida. O receptor calcula $h(m')$ e compara este valor com $h(m)$, que também foi recebido. Se estes dois valores forem diferentes, então e mensagem foi alterada durante a transmissão. Caso contrário, a mensagem não foi alterada (com grande probabilidade).