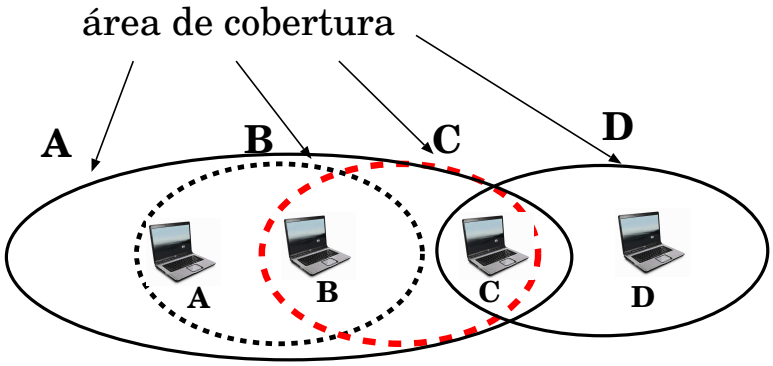
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
GABARITO da AP2 - 1° semestre de 2011

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.

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 D quer enviar uma mensagem para B, a mensagem passará por C até chegar a B.

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 B e D tenham mensagens para enviar para C.

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

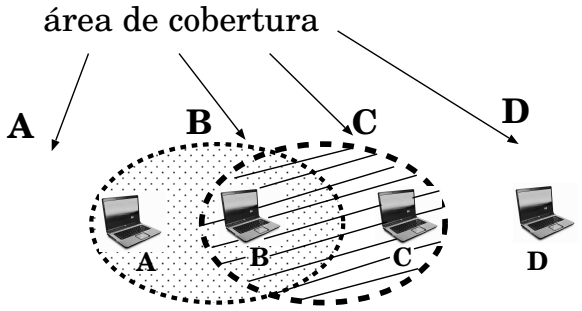
   Resposta: Não, pois a mensagem transmitida por B será recebida somente pelo terminal A para depois ser retransmitida para C. Enquanto que a mensagem transmitida por D será diretamente recebida por C.

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

Resposta: Não, pois B não está na área de cobertura de D.

2. (0.5) Considere agora que em um slot de tempo, B tem uma mensagem para enviar para A e C tem uma mensagem para enviar para D. Neste caso irá ocorrer uma colisão ? Explique porquê.

   Resposta: Não, pois neste caso B estará transmitindo sua mensagem para A (que não está na área de cobertura de C) e C estará transmitindo sua mensagem para D. (B estará recebendo a transmissão de C mas isso não atrapalha sua transmissão). Como a transmissão de C não chega até A, A receberá a mensagem de B sem problemas. D não está na área de cobertura nem de C nem de B, portanto não receberá nenhuma das duas mensagens. A figura abaixo ilustra a área de transmissão das duas mensagens, mostrando que A recebe somente uma mensagem e D não recebe nenhuma.



3. Suponha que A envie uma mensagem destinada a D, e que nenhum outro terminal vá transmitir mensagens até que a mensagem chegue em D.

   (a) (0.5) 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 é de zero mensagens por slot de tempo pois D não está na área de cobertura de nenhum outro terminal da rede.

   (b) (0.5) Por quais terminais a mensagem irá passar até chegar ao seu destino ?

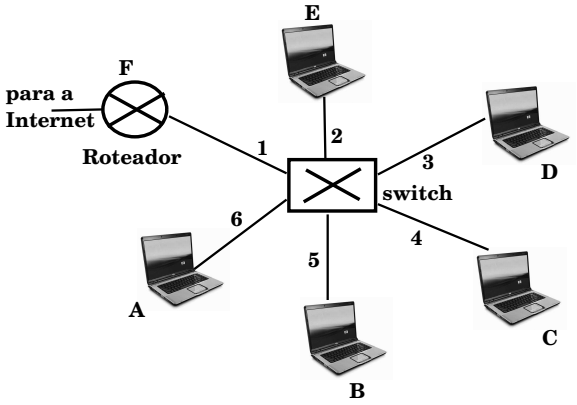
   Resposta: A mensagem é transmitida de A para B e C mas D não está na área de cobertura de nenhum outro terminal, portanto ele não pode receber mensagens de outro terminal desta rede. D só pode enviar mensagens para os outros terminais.

4. (0.5) Descreva um cenário onde duas estações podem transmitir simultaneamente sem que ocorra uma colisão.

   Resposta: D para C e B para A.

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) A envia uma mensagem para E.

   Resposta:

endereço	Interface
A	6

   A mensagem será encaminhada por todas as interfaces exceto a interface 6.

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

   Resposta:

endereço	Interface
A	6
E	2

   A mensagem será encaminhada por todas as interface exceto a interface 2.

3. (0.5) D envia uma mensagem para A.

   Resposta:

endereço	Interface
A	6
E	2
D	3

   A mensagem será encaminhada pela interface 6.

4. (1.0) Descreva brevemente como funciona o algoritmo de aprendizado usado pelo switch para encaminhar as mensagens e montar a sua tabela de encaminhamento.

   Resposta

   Quando um switch recebe um quadro, procura o endereço MAC de destino na sua tabela

   Se encontrar o endereço na sua tabela

   então {se o endereço de destino está no mesmo segmento de LAN de onde o quadro chegou}

   então {descarta o quadro}

   senão {encaminha o quadro na interface indicada na tabela}

   senão {encaminha o quadro por todas as interfaces de saída exceto pela interface por onde recebeu o quadro}

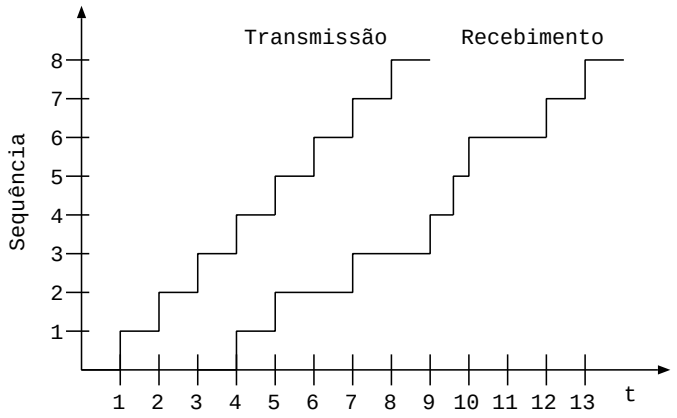
Suponha que todos os links que interconectam os computadores com o switch são de 100 Mbps e que o link que interconecta o switch com o roteador é de 10 Gbps.

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 500 Mbps.

$3^{\underline{a}}$ 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: Seja T_i e R_i o tempo de transmissão e recebimento do pacote i, respectivamente. Temos então que $T_1 = 1$, $T_2 = 2$, $T_3 = 3$, $T_4 = 4$, $T_5 = 5$, $T_6 = 6$, $T_7 = 7$, $T_8 = 8$. Temos também que $R_1 = 4$, $R_2 = 5$, $R_3 = 7$, $R_4 = 9$, $R_5 = 9.5$, $R_6 = 10$, $R_7 = 12$, $R_8 = 13$.

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

   Resposta: Seja A_i o retardo (ou atraso) sofrido pelo pacote i. Temos então que $A_i = R_i - T_i$, uma vez que o retardo é dado pela diferença do instante de recebimento e do instante de transmissão. Assim sendo, temos que $A_1 = 3$, $A_2 = 3$, $A_3 = 4$, $A_4 = 5$, $A_5 = 4.5$, $A_6 = 4$, $A_7 = 5$, $A_8 = 5$.

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 chegada do primeiro pacote, todos os pacotes que sofrerem um atraso maior do que o primeiro serão descartados pois não chegarão no instante em que deveriam ser decodificados. Desta forma, todos os pacotes com exceção do 1 e 2 seriam perdidos, pois todos os outros tem um retardo maior do que 3.

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 iniciar duas unidades de tempo depois da chegada do primeiro pacote, então podemos tolerar um atraso de $3 + 2 = 5$ unidades de tempo. Desta forma, todos os pacotes que tiverem atraso maior do que cinco serão perdidos. No caso acima, nenhum pacote será perdido, pois todos possuem retardo menor ou igual a 5.

$4^{\underline{a}}$ 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. Ana nunca deve revelar sua chave privada, nem mesmo a Bruno!

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

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

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

   (e) Bruno não precisa conhecer nenhuma chave de Ana para receber m com confidencialidade.
   Resposta: Verdadeiro. Apenas Ana precisa conhecer a chave pública de Bruno para que ela possa enviar m de forma confidencial.

2. (0.5 pontos) Explique o que é a propriedade de *não-repudiação* garantida por assinaturas digitais. Descreva como esta propriedade é garantida (dê um exemplo).

   Resposta: Não-repudiação significa que uma pessoa não pode negar que uma determinada assinatura digital não é sua. Ou seja, ao assinar um documento digitalmente, não podemos depois negar o fato. Esta propriedade é garantida utilizando chave pública/privada de uma entidade A, ou seja K_A^+, K_A^-. Para assinar o documento m ciframos o documento com a chave privada, obtendo $K_A^-(m)$. Para verificar a assinatura ciframos o documento assinado com a respectiva chave pública, obtendo $K_A^+(K_A^-(m)) = m$. Repare que apenas a chave pública associada a chave privada irá gerar m de volta. Como a chave privada é de conhecimento apenas de A, temos certeza de que ele foi assinado por A e por mais ninguém. Desta forma, A não pode refutar que assinou o documento m.

3. (0.5 pontos) Explique por que é importante que seja difícil inverter uma função de hash utilizada para gerar *message digests* (resumo). Ou seja, por que é importante ser difícil descobrir algum M dado $H(M)$.

   Resposta: *Message digests* são utilizados para garantir a integridade dos dados. Ou seja, desejamos detectar se uma determinada mensagem M foi modificaca durante sua transmissão. Seja $H(M)$ o message digest de M. Se for fácil inverter a função H, então podemos obter uma outra mensagem M' para a qual $H(M') = H(M)$, ou seja, tanto M quanto M' possuem o mesmo *message digest*. Neste caso, poderíamos trocar M por M' sem que isto fosse detectado pelo receptor, uma vez que os message digests são idênticos. Por isto, deve ser muito difícil encontrar uma mensagem M' qualquer dado um $H(M)$ qualquer.