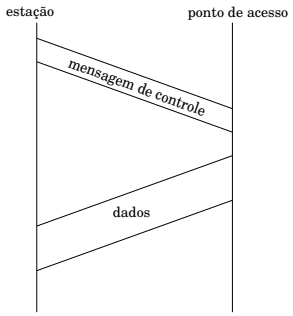
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 1° semestre de 2013

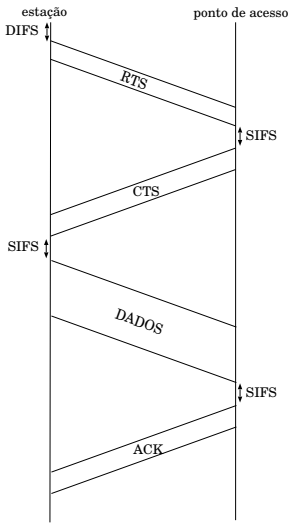
1ª questão (3.0 pontos)

Considere uma rede operando o protocolo IEEE 802.11 no modo com reserva, ou seja, usando os quadros RTS/CTS. Suponha que uma estação queira transmitir um quadro de 1000 bytes e todas as outras estações estejam ociosas neste instante.

1. (1.0) Faça um diagrama temporal (semelhante ao exemplo abaixo), ilustrando a troca de mensagens entre a estação e o ponto de acesso 802.11. Inclua todas as mensagens trocadas e os tempos entre as mensagens, desde a primeira mensagem enviada pela estação para reserva do canal até o recebimento do ACK.



Resposta:



2. (1.0) Calcule o tempo total que a estação levará para trasnmitir o quadro e receber o ACK. Inclua todos os tempos e mensagens de controle envolvidos na transmissão (como no item acima) e considere a velocidade do canal igual a 10Mbps.

   Resposta:

   $tempo_{total} = t_{DIFS} + 3 * t_{SIFS} + t_{RTS} + t_{CTS} + t_{ACK} + \frac{1000*8}{10*10^6}$

3. (0.5) Descreva uma vantagem do uso dos quadros RTS/CTS.

   Resposta:

   Uma vantagem é diminuir o tempo de colisão pois as estações só irão colidir durante o tempo de transmissão desses quadros que tem tamanho pequeno.

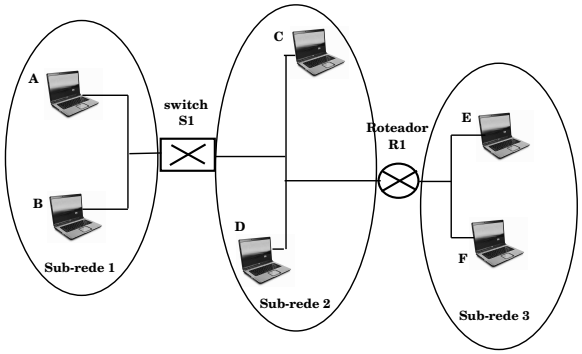
4. (0.5) Considerando que os quadros RTS/CTS tem tamanho igual a 20 bytes, descreva um cenário onde o uso desses quadros não seria eficiente.

   Resposta:

   O uso do RTS/CTS não seria eficiente caso o tamanho dos quadros de dados fosse aproximadamente igual ao tamanho dos quadros RTS/CTS. Neste cenário, o tempo de colisão dos quadros (dados e RTS/CTS) seria praticamente o mesmo e ainda haveria o overhead introduzido pelos quadros RTS/CTS.

$2^{\underline{a}}$ questão (3.0 pontos)

Interconexão de redes



Considere o cenário da figura acima onde um switch S1 interconecta as sub-redes 1 e 2 e um roteador R1 interconecta as sub-redes 2 e 3. Responda as perguntas abaixo, justificando as suas respostas:

1. (0.5) Considere que o computador E queira enviar um datagrama IP para F. O computador E irá solicitar a R1 para enviar o datagrama ? Por quê ?

   Resposta:

   Não, pois quando E fizer um AND do IP destino (F) com a máscara de rede, irá descrobrir que F está na mesma sub-rede que ele e portanto ele não precisa usar R1 para encaminhar o datagrama.

2. (1.0) Suponha que E queira enviar um datagrama IP para B e que a tabela ARP de E não contenha o endereço MAC de B. Que mensagens do protocolo ARP devem ser enviadas/recebidas por E para que o datagrama seja transmitido para B ?

   Resposta:

Passo 1: E envia pacote ARP query em broadcast contendo endereço IP de R1 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 R1.

Passo 2: R1 recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de E.

Passo 3: E recebe o pacote de R1 e atualiza a sua tabela ARP criando uma entrada com o endereço IP de R1 e o respectivo MAC. E envia quadro cujo endereco MAC de destino é o MAC de R1. Neste quadro, E encapsula o pacote destinado a B (IP destino é B).

Passo 4: Quando R1 receber o quadro enviado por E, ele usará o IP destino de B para descobrir por qual interface deve encaminhá-lo. R1 descobrirá que deve encaminhá-lo através da interface que o liga a S1.

Passo 5: Quando S1 receber o pacote, ele o encaminhará através da porta que o liga a B.

3. (1.5) Considere que A quer enviar um datagrama IP para B e nem A possui o MAC de B e nem B possui o MAC de A. Suponha também que a tabela de encaminhamento do switch S1 contém entradas para o computador B e o roteador R1.

   (a) (0.3) Que mensagem A enviará para obter o MAC de B ?
   Resposta:
   A enviará uma mensagem ARP query em broadcast contendo o endereço IP de B.

   (b) (0.3) O que S1 fará quando receber a mensagem de A ?
   Resposta:
   S1 enviará a mensagem ARP query por todas as interfaces exceto a interface pela qual ele recebeu a mensagem. S1 atualizará sua tabela inserindo o MAC de A e sua respectiva interface.

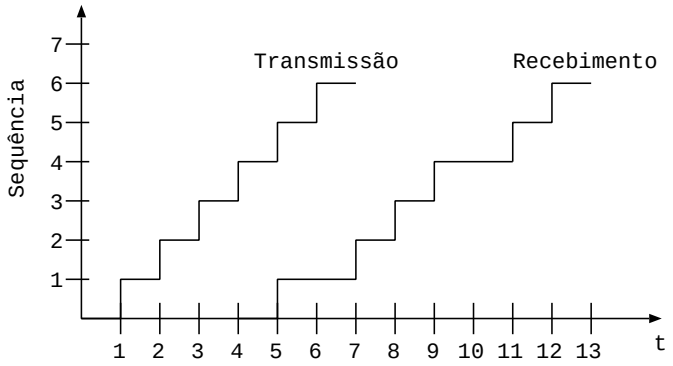
   (c) (0.3) O roteador R1 vai receber essa mensagem ? Se sim, ele vai encaminhá-la na sub-rede 3 ?
   Resposta:
   Sim, R1 recebe a mensagem mas não encaminha através da sub-rede 3.

   (d) (0.3) Quando B receber a mensagem de A, B irá responder. O que S1 fará quando receber a resposta de B ?
   Resposta:
   S1 enviará a mensagem pela interface que o liga a A.

   (e) (0.3) Quais serão as entradas da tabela de encaminhamento de S1 após a troca das mensagens ?
   Resposta:
   MAC A - interface
   MAC B - interface
   MAC R1 - interface

3ª 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: $T_1 = 1$, $R_1 = 5$, $T_2 = 2$, $R_2 = 7$, $T_3 = 3$, $R_3 = 8$, $T_4 = 4$, $R_4 = 9$, $T_5 = 5$, $R_5 = 11$, $T_6 = 6$, $R_6 = 12$.

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: $A_1 = 4$, $A_2 = 5$, $A_3 = 5$, $A_4 = 5$, $A_5 = 6$, $A_6 = 6$.

3. (0.5) Assuma agora que a decodificação dos pacotes pelo cliente irá iniciar **uma unidade 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:

   Caso o cliente inicie uma unidade de tempo depois, ele precisará dos pacotes nos seguintes instantes: $6, 7, 8, 9, 10, 11$. Logo, os pacotes 5 e 6 serão perdidos pois chegarão uma unidade de tempo depois do instante que deveriam ser tocados.

4. (0.5) Qual o tamanho mínimo do buffer para que nenhum pacote seja perdido ?

   Resposta:

   O tamanho mínimo é igual a duas unidades de tempo pois, com este buffer, os pacotes seriam tocados nos instantes: $7, 8, 9, 10, 11, 12$. Neste cenário, todos os pacotes já teriam sido recebidos.

$4^{\underline{a}}$ 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).