

Fundação CECIERJ - Vice Presidência de Educação Superior a Distância
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 1º semestre de 2012

1ª questão (1.5 pontos)

Complete a tabela abaixo indicando com um **X** se um determinado equipamento de interconexão de rede possui uma certa propriedade ou não. Justifique resumidamente as suas respostas.

	roteador	hub	switch
isola tráfego	X		X
não necessita de configuração		X	X
roteamento ótimo	X		
estações compartilham o mesmo domínio de colisão		X	

2ª questão (1.0 ponto)

Descreva o que são os seguintes problemas encontrados em uma rede sem fio: propagação multicaminho e interferência de outras fontes.

Resposta:

propagação multicaminho : É o fato do mesmo sinal emitido por uma determinada fonte chegar no destino em instantes distintos de tempo pois foi refletido por outros objetos (ex: montanha, avião, etc) no seu trajeto entre a fonte e o destino.

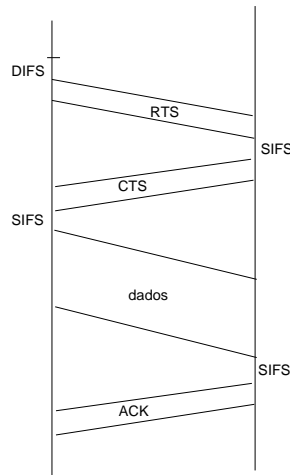
interferência de outras fontes : As frequências padronizadas para redes sem fio são compartilhadas por outros equipamentos. Motores também produzem interferência.

3ª questão (1.5 pontos)

Considere uma estação conectada a uma rede IEEE802.11 que está configurada para operar com reserva de canal (mensagens RTS/CTS). Suponha que esta estação tenha que enviar 1000 bytes de dados no instante t e que todas as estações estejam ociosas neste momento. Considere que não houve erro na transmissão da mensagem.

1. (0.8) Construa um diagrama temporal das mensagens trocadas entre as estações origem e destino até que um ACK seja recebido. Considere todas as mensagens/tempos envolvidos na transmissão com sucesso da mensagem de 1000 bytes (RTS, CTS, SIFS, DIFS). (Veja abaixo um exemplo do tipo de diagrama a ser elaborado.)

Resposta:



2. (0.7) Suponha que a capacidade de transmissão do canal é de 2Mbps/s. Calcule o tempo desde que a estação origem inicia o processo para transmitir a mensagem de 1000 bytes até que a mensagem seja recebida na estação destino (este tempo deve incluir as mensagens de sinalização/tempo envolvidos na transmissão).

Resposta:

$$tempo = (1000 * 8 / 2 * 10^6) + RTS + CTS + DIFS + (2 * SIFS) = 4 * 10^{-3} + RTS + CTS + (2 * SIFS)$$

4ª questão (4.0 pontos)

Aplicações multimídia. Responda às perguntas abaixo.

1. (0.5) Explique o que é o jitter na Internet.

Resposta:

Jitter é a variação do atraso. Suponha que pacotes são transmitidos na Internet de um host A para um host B. Considere que o atraso do pacote i é r_i e o atraso do pacote $i+1$ é r_{i+1} , o jitter é dado por $r_{i+1} - r_i$.

2. (0.5) Explique porque o jitter pode prejudicar a qualidade de aplicações de vídeo e voz na Internet.

Resposta:

Um dos requisitos das aplicações de vídeo e voz é que os pacotes sejam entregues no destino com o mesmo intervalo de tempo que foram gerados na origem. O jitter pode alterar este intervalo entre pacotes.

3. O buffer é um exemplo de um mecanismo para minimizar o jitter. Suponha que o buffer escolhido para uma certa aplicação tem um tamanho B . Cite uma vantagem e uma desvantagem para os seguintes casos:

- (a) (0.5) B é igual a 2 pacotes de dados.

Resposta:

Vantagem: Entrega rápida de pacotes para a aplicação.

Desvantagem: Se a rede possui um atraso que varia muito no tempo, um número grande de pacotes pode não ser entregue a aplicação pois os mesmos chegariam após o momento que deveriam ter sido tocados.

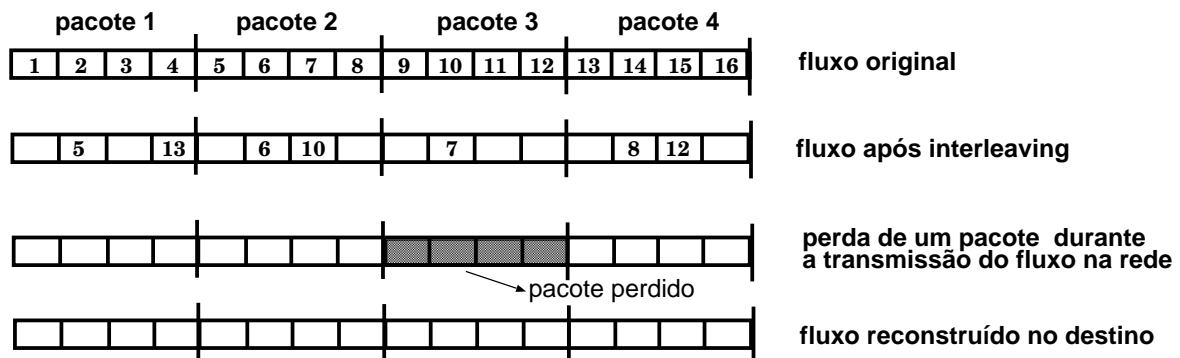
- (b) (0.5) B é igual a 10 pacotes de dados.

Resposta:

Vantagem: Se a rede possui um atraso que varia muito no tempo, um buffer de 10 pacotes é uma forma de *compensar* esta variação, aumentando a chance de pacotes com valores de jitter bem diferentes poderem ser entregues a aplicação.

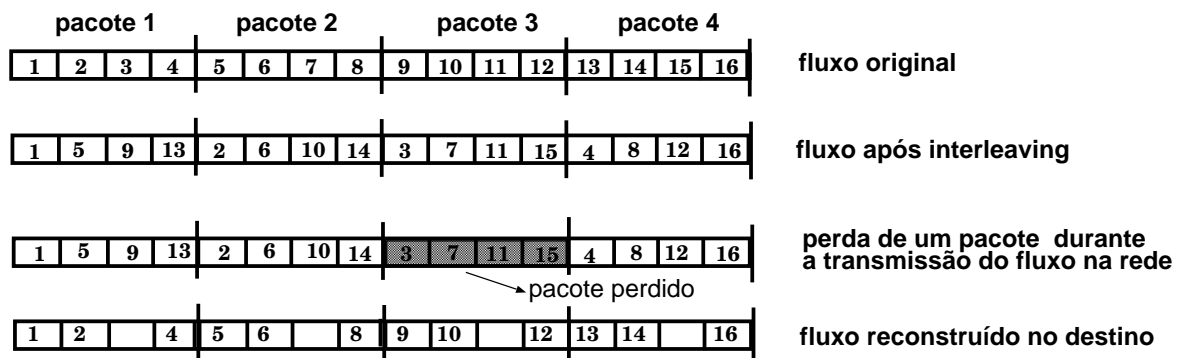
Desvantagem: Retardo para iniciar a aplicação pode ser alto.

4. Considere a figura abaixo onde pacotes são enviados usando a técnica de interleaving na transmissão de um fluxo na Internet.



- (a) (1.0) Complete os retângulos em branco da figura com os números dos blocos que compõe um pacote. Use a técnica de interleaving.

Respsota:



- (b) (0.6) Cite uma vantagem e uma desvantagem desta técnica.

Resposta:

Vantagem: Não possui overhead devido a informação redundante transmitida na rede.

Desvantagem: Tempo para remontar pacotes no destino pode ser alto.

- (c) (0.4) Para o exemplo da figura, qual o atraso para entrega de um pacote para a aplicação a partir da chegada do primeiro bloco deste pacote ?

Resposta:

O atraso é de 12 blocos.

5ª questão (2.0 pontos)

Segurança em redes. Responda às perguntas abaixo.

1. (0.5) Considere um *firewall* que permite que os computadores que estejam dentro da rede protegida enviem email. Ou seja, o firewall possui uma regra que encaminha corretamente pacotes do protocolo TCP com porta 25 provenientes de computadores da rede protegida. Considere agora um outro aplicativo qualquer (ex. Kazaa) que utiliza o mesmo protocolo e porta para se comunicar. Os pacotes gerados por tal aplicativo serão descartados pelo firewall? Explique sua resposta.

Resposta:

Não, pois pela regra do firewall ele deixará passar pacotes TCP provenientes da porta 25 independente da aplicação que esteja usando a porta.

2. (0.5) Explique o que é *IP Spoofing*. Explique por que *IP Spoofing* pode levar a um problema de segurança.

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) 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 mensagem. 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 realizar para ler a mensagem recebida.

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 mensagem.
- 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 .