Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 - GABARITO - 1° semestre de 2008

Nome:

Assinatura:

Observações:
1.Prova sem consulta e sem uso de máquina de calcular.
2.Use caneta para preencher o seu nome e assinar nas folhas de questões e nas folhas de respostas.
3.Você pode usar lápis para responder as questões.
4.Ao final da prova devolva as folhas de questões e as de respostas.
5.Todas as respostas devem ser transcritas nas folhas de respostas. As respostas nas folhas de questões não serão corrigidas.

1ª questão (2.0 pontos)

Aplicações multimídia na Internet tendem a transmitir informação redundante juntamente com o fluxo de dados original.

1. (0.5 ponto) Qual é o objetivo desta redundância?

   Resposta:

   O objetivo de enviar redundância é recuperar pacotes que tenham sido descartados pela rede. Ou seja, recuperar pacotes que não chegaram ao seu destino sem fazer retransmissão.

2. (0.5 ponto) Cite ao menos uma vantagem e uma desvantagem de transmitir informação redundante.

   Resposta:

   Uma vantagem é que a recuperação é feita sem a necessidade de retransmissão dos pacotes, o que significa que os pacotes pode ser recuperados (ou seja, reconstruídos) mais rapidamente. Uma desvantagem é o envio de informação desnecessária, no caso da rede não descartar os pacotes, consumindo desnecessariamente recursos da rede.

3. (1.0 ponto) Descreva como funciona o mecanismo de redundância (FEC) simples baseado em OU-Exclusivo. Dê um exemplo ilustrando este mecanismo.

Resposta:

O mecanismo funciona com janelas de pacotes, por exemplo com janelas com n pacotes. O mecanismo então calcula o ou-exclusivo dos n pacotes de uma janela, gerando um novo pacote, que é o pacote redundante. Este novo pacote é a transmitido após os n pacotes da janela. Se um dos pacotes da janela for descartado pela rede, então este pacote é reconstruído fazendo o ou-exclusivo dos outros $n-1$ pacotes e do pacote redundante. Se mais de um pacote de uma janela for descartado, então o mecanismo não consegue recuperá-los.

2ª questão (1.0 ponto)

Aplicações multimídia na Internet, especialmente aplicações com *streaming*, tendem a utilizar a técnica de bufferização do lado do cliente.

1. (0.5 ponto) Qual é o objetivo desta bufferização?

   Resposta:

   O objetivo desta bufferização é diminuir a variância do atraso dos pacotes para a aplicação. Ou seja, permite a aplicação consumir os pacotes de forma mais suave, sem que haja interrupções no consumo dos dados.

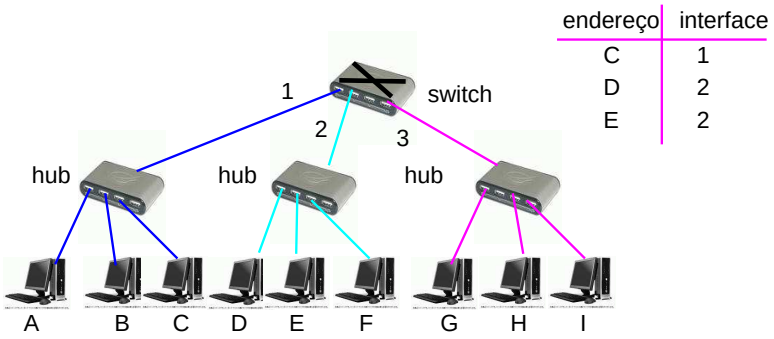
2. (0.5 ponto) Discuta ao menos uma vantagem e uma desvantagem da bufferização.

   Resposta:

   Uma vantagem é justamente oferecer uma melhor qualidade de vídeo ou áudio ao usuário, pois mascara os atrasos da rede. Uma desvantagem é prejudicar a interatividade, fazendo com que o usuário tenha que aguardar um tempo antes do conteúdo ser apresentado.

3ª questão (2.5 pontos)

Considere na rede abaixo que o *host* E quer enviar uma mensagem para G. Os hosts E e G estão interconectados através de um switch que possui a tabela de encaminhamento mostrada na figura abaixo.



1. (0.6) Suponha que E envie uma mensagem para G. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? (Explique porque). Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

   Resposta:

   Quando a mensagem enviada por E chega no switch não ocorre nenhuma atualização na tabela pois E já se encontra na tabela do switch.

O switch encaminha a mensagem pelas interfaces 1 e 3 pois G não consta da sua tabela.

2. (0.6) Agora suponha que G envie uma mensagem (resposta) para E. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? (Explique porque). Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

   Resposta:

   Quando a mensagem enviada por G chega no switch, ele cria uma entrada associando G a interface 3.

   O switch encaminha a mensagem pela interface 2 pois esta é a interface associada com E que consta da sua tabela.

3. (0.6) Descreva duas vantagens de switches sobre hubs.

   Resposta:

   1 - Switches isolam tráfego, ou seja, máquinas conectadas em portas diferentes não colidem pois estão em domínios de colisão distintos.

   2 - Switches possuem buffer e portanto podem conectar máquinas com interfaces de rede de velocidades diferentes.

   3 - Switches usam um algoritmo de encaminhamento que permite o envio do tráfego por uma única interface (aquela onde se encontra a máquina destino) ao invés do envio por todas as interfaces.

4. (0.7) Explique resumidamente como funciona o algoritmo de encaminhamento dos switches.

   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

4ª questão (1.5 pontos)

Considere a figura abaixo como sendo a rede de uma instituição.

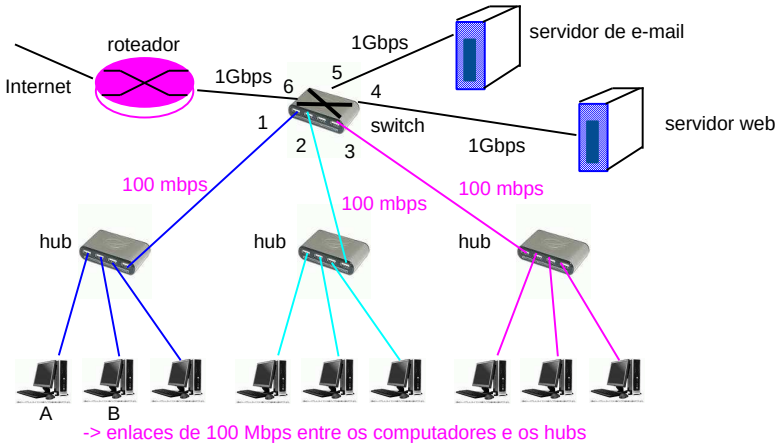
1. (0.6) Qual a vazão (bits por segundo) máxima agregada que pode ser alcançada entre o conjunto composto por todos os computadores que estão conectados aos hubs e a internet.

   Resposta

   A vazão máxima é 300Mbps.

2. (0.9) Suponha que o computador A queira enviar uma mensagem ao computador B mas não possua o endereço MAC de B. Qual o protocolo deve ser usado para que A obtenha o endereço MAC de B e que mensagens devem ser trocadas entre A e B até que A obtenha o MAC de B ?

   Resposta



O protocolo que deve ser usado é o ARP.

Passo1: A envia pacote ARP query em broadcast contendo endereço IP de B.

Passo2: B recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de A.

Passo3: A recebe o pacote de B e atualiza a sua tabela ARP criando uma entrada com o endereço IP de B e o respectivo MAC.

5ª questão (1.0 ponto)

O padrão IEEE802.11 tem dois modos de operação: com e sem reserva. Suponha os seguintes cenários: (i) o tamanho médio do quadro de dados é 3 vezes maior que o tamanho do quadro de reservas e (ii) o tamanho médio do quadro de dados é pouco maior que o tamanho do quadro de reservas. Qual modo de operação você escolheria para cada um dos cenários ? (Explique os motivos da sua escolha.)

Resposta:

Cenário (i) : Escolheria o protocolo com reserva. Neste caso como o tamanho médio do quadro de dados é bem maior do que o quadro de reserva, o overhead introduzido pelos quadros de reserva é menor do que o tempo que duraria a colisão de quadros de dados.

Cenário (ii) : Escolheria o protocolo sem reserva. Neste caso como o tamanho médio do quadro de dados é pouco maior que o tamanho do quadro de reservas, o overhead introduzido pelos quadros de reserva é maior que o tempo que duraria a colisão de quadros de dados.

6ª questão (2.0 pontos)

Segurança em Redes: Responda às perguntas abaixo.

1. (0.5 ponto) Descreva como funciona criptografia com chave pública/privada. Qual é a grande diferença desta abordagem quando comparada à criptografia com chave simétrica?

   Resposta:

   Criptografia com chave público/privada funciona da seguinte maneira. Uma entidade gera um par de chaves, uma publica e outra privada. A chave publica é anunciada publicamente e distribuida para todos que desejam se comunicar com a entidade de forma segura. A chave privada é mantida em sigilo. A chave publica é então usada para cifrar os dados que precisam ser transmitidos para a entidade, que então são decifrados

com a chave privada. A principal diferença com criptografica com chave simétrica está no uso de um par de chaves, uma pública e outra privada.

2. (0.5 ponto) Explique porque o uso de um *nonce* evita o ataque de playback durante o processo de autenticação.

   Resposta:

   O ataque de playback não funciona pois o nonce é único e diferente para cada processo de autenticação. Ou seja, a entidade que está autenticando gera um novo número que precisa ser criptografado e enviado de volta. Como este número é diferente para cada autenticação, o ataque de playback não irá funcionar.

3. (1.0 ponto) Descreva como funciona um *firewall* baseado em pacotes. Uma rede protegida por um *firewall* pode ser "invadida"? Discuta sua resposta.

   Resposta:

   Um firewall baseado em pacotes funciona verificando cada pacote que chega contra um conjunto de regras. Ou seja, cada pacote que chega ao roteador (firewall), é inspecionado para decidir se o mesmo deve ou não ser encaminhado pelo roteador. Tal decisão é feita com base em regras (filtros) definidas pelo administrador da rede. Estas regras geralmente utilizam informacoes no cabeçalho do pacote.

   Sim. Uma rede protegida por um firewall pode ser invadida, ainda mais quando "invasão"significar ter pacotes indesejados trafegando pela rede protegida. Repare que um firewall filtra pacotes baseado em regras pré-estabelecidas, o que não impossibilita que todos os pacotes indesejados trafeguem pela rede. O problema principal é saber quais pacotes são indesejados, quais pacotes devem ser filtrados.