Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 2° semestre de 2010

1ª questão (2.0 pontos)

1. (1.0) Explique o que são as características de enlaces sem fio: propagação multicaminho e diminuição da potência do sinal. Por que elas podem dificultar a transmissão com sucesso ?

   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.

   diminuição da potência do sinal : É o fato do sinal perder a sua potência a medida que se propaga no meio livre ou atravessa objetos.

   As características acima aumentam a taxa de erro em redes sem fio quando comparada com a taxa em redes com fio. Além disso as taxas de erros podem variar muito ao longo do tempo devido ao movimento dos objetos e dos terminais móveis.

2. (1.0) Explique resumidamente como funciona o protocolo IEEE 802.11.

   Resposta:

   O protocolo IEEE802.11 é baseado no algoritmo CSMA/CA definido para acesso ao meio de transmissão. Ele possui dois modos principais de operação: com reserva e sem reserva. Os modos com e sem reserva estão descritos abaixo.

   - Modo sem reserva (protocolo CSMA/CA):
     - Emissor 802.11:
       Passo 1: se o canal estiver livre, espera um pequeno tempo (DIFS) e então transmite todo o quadro
       Passo 2: se o canal estiver ocupado então
       - inicia um tempo de backoff aleatório
       - decrementa o tempo de backoff quando o canal estiver livre
       - transmite quando o tempo de backoff chegar a zero
       - se não chegar um ACK, aumenta o tempo de backoff e repete o passo 2
     - Receptor 802.11:
       se o quadro recebido estiver OK
       - envia ACK depois de esperar um tempo pequeno chamado SIFS
   - Modo com reserva:
     - Emissor primeiramente envia pequenos pacotes de controle *Resquest to Send* (RTS) para o AP usando o protocolo CSMA/CA descrito acima.

– AP envia um pacote *Clear to Send* (CTS) em resposta a um RTS recebido.
– CTS é recebido por todas as estações que estão ao alcance do AP.
– Emissor transmite o quadro de dados após recebimento do CTS.
– Outras estações bloqueiam suas transmissões durante a trasnmissão do quadro de dados da estação que recebeu o CTS. Com isso, não ocorrem colisões de quadros de dados, as colisões só ocorrem entre pacotes de controle.

2ª questão (2.0 pontos)

1. (1.0) Explique 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

2. (1.0) Descreva uma vantagem e uma desvantagem que switches possuem com relação a hubs.

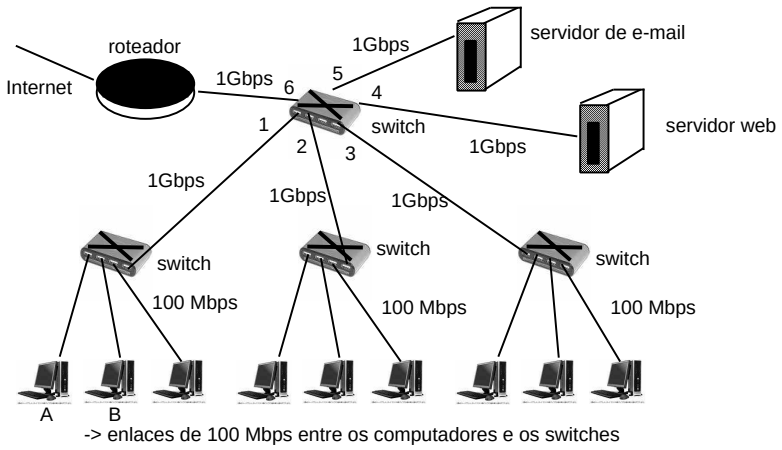
   Resposta

   Vantagem: (i) Switches podem interconectar redes com velocidades diferentes pois possuem buffer; (ii) Switches isolam domínios de colisão.

   Desvantagem: Hubs por serem simples repetidores podem ser mais rápidos que switches.

3ª questão (2.0 pontos)

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



1. (0.4) Qual a vazão (bits por segundo) máxima agregada que pode ser alcançada entre a rede da instituição e a internet. Justifique a sua resposta.

   Resposta:

   A vazão máxima é de 1 Gbps pois esta é a velocidade do link entre o switch e a Internet.

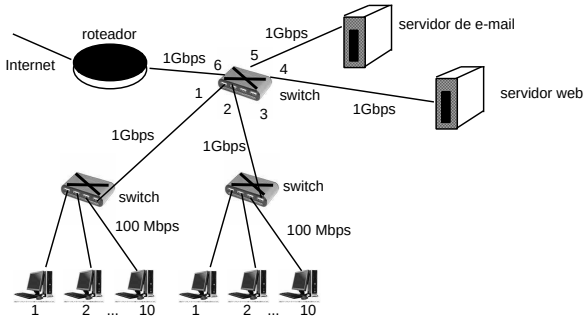
2. (0.4) Caso as portas de 100 Mbps fossem substituídas por portas de 1Gbps qual seria a nova vazão entre a rede da instituição e a internet ? Justifique a sua resposta.

   Resposta: A vazão continuaria sendo 1 Gbps pois esta é a velocidade do link entre o switch e a Internet.

3. (0.5) Suponha que você seja contratado para definir a arquitetura da rede da instituição de forma a atender aos seguintes requisitos: (i) cada cliente deve poder acessar uma aplicação de vídeo de até 50 Mbps; (ii) cada switch deve atender no mínimo 10 clientes. Qual a configuração **mínima** da rede projetada por você para atender os requisitos acima ?

   Resposta:

   Cada switch deve conter 10 portas de 100 Mbps, cada uma sendo usada para atender cada um dos 10 clientes, e uma porta de 1 Gbps ligando o switch do cliente ao switch que está ligado ao roteador. A figura abaixo ilustra um projeto para esta rede. Note que não é possível ter mais do que dois switches com clientes pois os requisitos de vídeo poderiam não ser atendidos.



4. (0.7) Suponha que um computador A da rede da instituição tenha que encaminhar uma mensagem para um computador B localizado na mesma rede local. Qual protocolo deve ser usado para que A descubra o endereço MAC de B ? Que mensagens devem ser trocadas para que A obtenha o MAC de B ?

   Reposta:

   O protocolo que deve ser usado é o ARP.

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

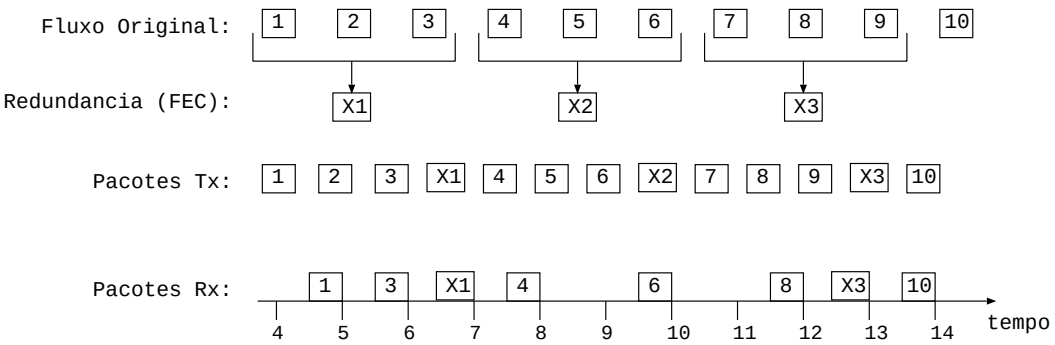
   Passo2: B recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de A.

   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.

4ª questão (2.0 pontos)

Aplicações multimídia. Considere o diagrama abaixo que ilustra a transmissão de pacotes multimídia utilizando um mecanismo de redundância simples, ou seja, um mecanismo baseado em ou-exclusivo com tamanho de janela $n = 3$. A figura ilustra o fluxo de dados original, os pacotes com a redundância, a transmissão dos pacotes e o recebimento dos pacote. Responda às perguntas abaixo:

1. (0.6) Determine quais pacotes de dados são efetivamente perdidos. Ou seja, quais pacotes a aplicação não irá recuperar.



Resposta:

Os pacotes que são efetivamente perdidos são aqueles que não chegaram ao receptor e que não podem ser reconstruídos a partir da redundância. No caso o pacote 2 não chegou, mas pode ser reconstruído a partir de X1. Os pacotes 5, 7 e 9 não chegaram e não podem ser reconstruídos a partir da redundância. Assim sendo, estes são os pacotes que foram efetivamente perdidos.

2. (0.6) Determine quais pacotes descartados pela rede serão recuperados pelo mecanismo de redundância. Determine também o instante em que estes pacotes serão recuperados.

   Resposta:

   O único pacote perdido pela rede que será recuperado pelo mecanismo de redundância é o pacote 2. Este pacote será recuperado no instante de tempo 7, assim que chegar a redundância X1. Com este pacote de redundância e com os pacotes 1 e 3, podemos recuperar o pacote 2.

3. (0.8) Assuma agora que mecanismo de redundância utiliza uma janela de tamanho $n = 2$ e que exatamente os mesmos pacotes de dados são descartados pela rede, mas **todos** os pacotes com a redundância chegam ao receptor. Determine quais pacotes de dados são efetivamente perdidos neste caso. Ou seja, quais pacotes a aplicação não irá recuperar.

   Resposta:

   Os pacotes perdidos pela rede no exemplo acima foram os pacotes 2, 5, 7, 9. Com uma janela de tamanho $n = 2$ pacotes, todos estes pacotes serão recuperados, assumindo que todos os pacotes de redundância chegam ao receptor. Isto acontece porque não há perdas consecutivas nos pacotes perdidos e temos uma janela de tamanho 2. Por exemplo, o pacote 2 será recuperado através do pacote 1 e da redundância X1, o pacote 5 será recuperado através do pacote 6 e da redundância X3, e assim por diante.

$5^{\underline{a}}$ questão (2.0 pontos)

Segurança em redes. Considere as seguintes informações criptográficas disponíveis para Ana e Bruno:

- Seja K uma chave simétrica compartilhada entre Ana e Bruno.
- 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 $H(\cdot)$ uma função de *hash* utilizada para gerar *message digests* (resumos de mensagens).

- Seja m uma mensagem em texto que Ana deseja enviar a Bruno.

Responda às perguntas abaixo:

1. (1.0 ponto) O que Ana deve fazer para enviar m a Bruno de forma a garantir **apenas** a integridade da mensagem. Descreva os passos que Ana e Bruno precisam realizar utilizando as informações acima.

   Resposta:

   Para garantir apenas a integridade da mensagem Ana deve usar a função de *hash* e gerar um *message digest* da mensagem m, ou seja, Ana deve gerar $H(m)$. Além disso, para garantir que ninguém possa alterar a mensagem m e regerar um novo *message digest*, Ana deve cifrar o message digest gerado com a chave simétrica compartilhada com Bruno. Ou seja, Ana deve gerar $K(H(m))$. Ana então deve enviar m juntamente com $K(H(m))$ a Bruno.

   Bruno ao receber m' e $K(H(m))$, deve decifrar $K(H(m))$ usando a chave simétrica compartilhada com Ana, obtendo assim $H(m)$. Bruno deve então aplicar a função de *hash* à mensagem recebida m' e verificar se o message digest produzido, ou seja $H(m')$ é igual à $H(m)$ que foi decifrado. Caso negativo, a mensagem foi alterada durante a transmissão e deve ser descartada.

2. (1.0 ponto) O que Ana deve fazer para enviar m a Bruno de forma a garantir **apenas** a confidencialidade da mensagem. Descreva os passos que Ana e Bruno precisam realizar utilizando as informações acima.

   Resposta:

   Para garantir apenas a confidencialidade da mensagem, Ana deve cifrar a mensagem m usando a chave simétrica K compartilhada com Bruno, produzindo $K(m)$. Alternativamente, Ana pode usar a chave pública de Bruno (K_B^+) para cifrar a mensagem m, produzindo $K_B^+(m)$. Ana deve enviar uma destas mensagens cifradas a Bruno.

   Ao receber $K(m)$ de Ana, Bruno deve decifrar a mensagem usando a mesma chave simétrica K compartilhada com Ana, obtendo assim a mensagem m. Alternativamente, ao receber $K_B^+(m)$ de Ana ele deve decifrar esta mensagem usando sua chave privada K_B^-, obtendo assim $K_B^-(K_B^+(m)) = m$. Em ambos os casos, a confidencialidade, e apenas isto, estará garantida. Por exemplo, este procedimento não garante a integridade da mensagem nem a autenticidade (no caso de chave pública).