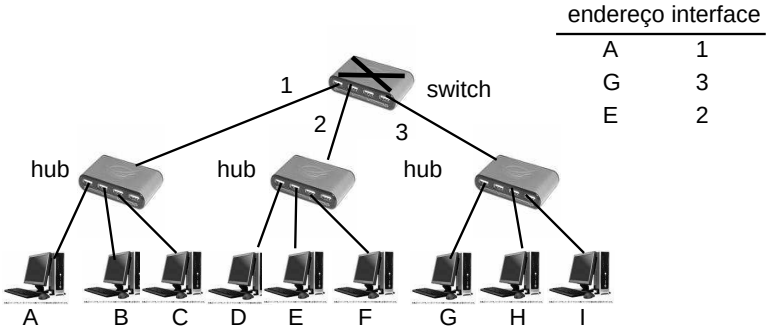
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 - GABARITO - 1° semestre de 2009

1ª questão (2.5 pontos)

Considere na rede abaixo que o *host B* envia uma mensagem para *o host F* e, em seguida, *F* responde à mensagem de *B*. Os hosts *B* e *F* estão interconectados através de um switch que possui a tabela de encaminhamento mostrada na figura abaixo.



1. (0.5) Por qual(is) interface(s) de saída do switch a mensagem do *host F* destinada ao *host B* será encaminhada ? (Explique porquê.)

   Resposta: Será encaminhada pela interface 1, pois o switch, após o envio da mensagem de B para F, criará uma entrada na tabela para o host B. Esta entrada foi inserida na tabela quando o host B enviou uma mensagem para F.

2. (0.5) Construa a tabela de roteamento do switch após a troca de mensagens entre *B* e *F*.

   Resposta:

endereço	interface
A	1
G	3
E	2
B	1
F	2

3. (0.5) Se ao invés de um switch, o equipamento usado para interconexão fosse um hub, por qual(is) interface(s) a mensagem de *B* para *F* seria encaminhada ? (Explique porquê.)

   Resposta:

   Seria encaminhada pelas interfaces 2 e 3 pois o hub é um simples repetidor: encaminha a mensagem por todas as interfaces de saída, exceto aquela pela qual recebeu a mensagem.

4. (0.5) Descreva um cenário em que pode ocorrer troca de mensagens entre hosts quaisquer e o switch não encaminhá-las por nenhuma de suas interfaces.

   Resposta:

   Esta situação ocorre quando um *host* envia uma mensagem para outro *host* que está no mesmo segmento de LAN, por exemplo, em uma troca de mensagens entre A e B.

5. (0.5) Cite duas características que diferenciam os switches de roteadores.

   Resposta:

   1 - Switches não implementam algoritmo para cálculo do melhor caminho de uma origem até um certo destino na rede. As tabelas de encaminhamento são geradas através de um algoritmo de aprendizado.

   2 - Switches não necessitam de intervenção de um administrador para entrarem em operação, são *plug and play*, diferentemente dos roteadores que necessitam ser configurados por um administrador.

2ª questão (1.5 pontos)

O padrão IEEE802.11 para redes locais sem fio tem dois modos de operação: com e sem reserva.

1. (0.7) 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 mé dio 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.

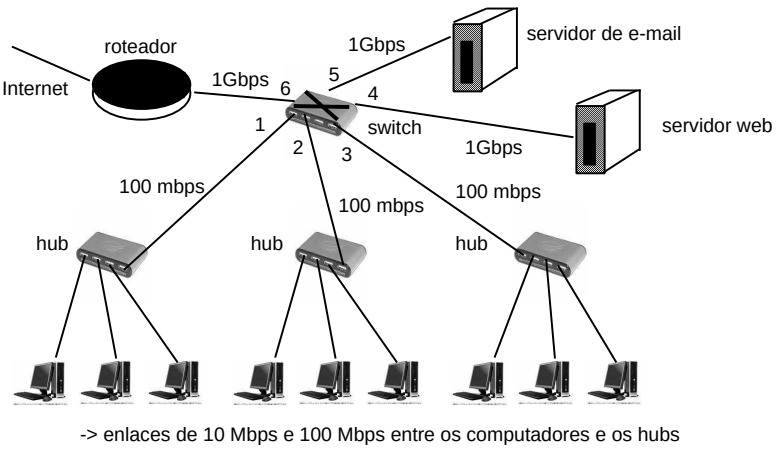
2. (0.8) Explique sucintamente como funciona o algoritmo de acesso ao meio deste protocolo para o caso de operação sem reserva.

   Resposta:

   - 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 SIFS

$3^{\underline{a}}$ questão (2.0 pontos)

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



1. (0.7 pontos) 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. Considere dois casos: que todos os computadores estão conectados ao hub a 10Mbps e a 100Mbps.

   Resposta:

   Caso 1: todos os computadores estão conectados ao hub a 10Mbps. A vazão máxima agregada entre o conjunto composto por todos os computadores que estão conectados aos hubs e a internet é igual a 90Mbps.

   Caso 2: todos os computadores estão conectados ao hub a 100Mbps. A vazão máxima agregada entre o conjunto composto por todos os computadores que estão conectados aos hubs e a internet é igual a 300Mbps.

2. (0.6 pontos) Quantos domínios de colisão existem na rede da instituição ? Se ao invés de hubs, tivermos switches, o número de domínios de colisão seria diferente ?

   Resposta:

   Existe um domínio de colisão para todos os computadores que estão conectados aos hubs. Se ao invés de hubs tivéssemos switches, cada conjunto de três computadores ligados ao switch estaria em um domínio de colisão diferente. Teríamos então três domínios de colisão um para cada grupo de três computadores.

3. (0.7 pontos) Considere duas modificações no cenário da figura acima: (i) substituição de hubs por switches e (ii) todas as portas do switch ligado ao roteador de 1Gbps. Neste novo cenário, qual seria a vazão (bits por segundo) máxima agregada que pode ser alcançada entre o conjunto composto por todos os computadores que estão conectados aos switches e a internet. Considere dois casos: que todos os computadores estão conectados ao hub a 10Mbps e a 100Mbps.

   Resposta:

   Caso 1: todos os computadores estão conectados ao hub a 10Mbps. A vazão máxima agregada entre o conjunto composto por todos os computadores que estão conectados aos switches e a internet é igual a 90Mbps. O fato de substituir hubs por switches e aumentar a velocidade das portas do switch não altera a vazão pois o gargalo é o enlace entre o computador e o switch que é de 10Mbps.

Caso 2: todos os computadores estão conectados ao hub a 100Mbps. A vazão máxima agregada entre o conjunto composto por todos os computadores que estão conectados aos switches e a internet é igual a 900Mbps. O gargalo neste caso passa a ser o enlace entre o computador e o switch que é de 100 Mbps.

4ª questão (2.0 pontos)

Considere o tipo de serviço oferecido pela Internet de hoje, conhecido como *best effort*. Responda às perguntas abaixo.

1. (0.4 pontos) O que difere fundamentalmente aplicações multimídia (ex. streaming de vídeo) das aplicações convencionais (ex. email)?

   Resposta:

   A diferença fundamental está nos requisitos destas aplicações. Aplicações multimídia são tolerantes a perdas esporádicas de dados mas não toleram bem a retardos introduzidos pela rede. Atrasos podem comprometer o uso da aplicação, enquanto perdas podem ser toleradas. Aplicativos convencionais possuem requisitos opostos, pois não toleram perdas de dados mas podem tolera bem atrasos introduzidos pela rede.

2. (0.4 pontos) Qual problema o mecanismo de bufferização do lado do cliente utilizado por aplicativos multimídia se propõe a resolver?

   Resposta:

   O objetivo do mecanismo de bufferização do lado do cliente é reduzir ou até mesmo eliminar o jitter introduzido pela rede. Lembrando que o jitter é a variação do atraso entre os pacotes do mesmo fluxo de dados.

3. (0.4 pontos) Qual é a desvantagem do mecanismo de bufferização do lado do cliente?

   Resposta:

   A grande desvantagem é o aumento do retardo de playback, ou seja, o usuário precisa aguardar mais tempo até que os dados comecem efetivamente a serem tocados. Isto se faz necessário, pois é preciso encher o buffer de alguns pacotes antes de iniciar a decodificação dos dados.

4. (0.4 pontos) Como aplicativos multimídia lidam com o fato de que usuários possuem acesso a Internet através de enlances com largura de banda distintas?

   Resposta:

   Basicamente oferecendo o conteúdo codificado em diferentes taxas, correspondendo a diferentes qualidades. Por exemplo, um mesmo vídeo pode ser disponibilizado em duas taxas, com mais e menos compressão, tendo menor e maior qualidade, respectivamente. Desta forma, usuários com largura de banda mais alta podem então acessar o vídeo de melhor qualidade, codificado com uma taxa maior.

5. (0.4 pontos) Por que aplicativos interativos em tempo real (ex. Skype) geralmente não utilizam a retransmissão de pacotes para recuperar pacotes perdidos?

   Resposta:

   Porque a retransmissão de pacotes em geral leva muito tempo, pois é preciso detectar a necessidade de uma retransmissão, solicitar a retransmissão a fonte, e receber o novo pacote. Este tempo é, geralmente, muito grande dado o curto espaço de tempo que aplicativos interativos possuem para receber e decodificar o áudio sem impactar a interatividade.

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

Segurança em redes. Responda às perguntas abaixo.

1. (0.4 pontos) Explique o que é a propriedade de *não-repudiação* garantida por assinaturas digitais e descreva como esta propriedade é garantida.

   Resposta:

   Não-repudiação significa que a pessoa que gerou e assinou uma determinada mensagem não pode negar este fato. Ou seja, se a mensgem M é assinada por A e transmitida a B, então A não pode negar que ele não gerou e assinou a mensagem. Esta propriedade é garantida com assinaturas digitais, da seguinte forma. Ao assinar M, A utiliza sua chave privada K_A^-. De posse da assinatura de M, qualquer um pode verificar que M foi foi assinada por A utilizando a chave pública de A, ou seja, K_A^+. Ninguém mais poderia ter assinado M, pois somente A tem conhecimento de sua chave privada K_A^-.

2. (0.4 pontos) Explique por que é importante que seja difícil inverter uma função de hash utilizada para gerar *message digests* (resumos). Ou seja, por que é importante ser difícil descobrir algum M dado $H(M)$.

   Resposta:

   Pois caso contrário seria fácil violar propriedades de segurança, como a integridade e até mesmo a não-repudiação. Por exemplo, se A deseja transmitir M para B sem que a mesma seja modificada, A pode enviar, por um meio seguro, $H(M)$ e por outro meio não seguro a mensagem M. Se for fácil inverter $H(M)$, o adversário pode encontrar uma outra mensagem M' tal que $H(M') = H(M)$ e substituir M por M' durante a transmissão. O receptor (B, neste caso) será enganado pois recebe M' e $H(M)$, e ao verificar constata que $H(M') = H(M)$. Entretanto, A transmitiu M e não M'.

Considere que Ana deseje enviar uma mensagem M para Bruno. Ana quer que a mensagem seja confidencial e que não seja modificada ao longo da transmissão. Ana adota o seguinte procedimento criptográfico:

1. Ana gera uma chave simétrica K que Bruno não conhece.
2. Ana cifra a mensagem M utilizando a chave simétrica K.
3. Ana cifra a chave simétrica K utilizando a chave privada de Bruno K_B^-
4. Ana envia a Bruno o resultado das operações 2 e 3 acima.

Responda às perguntas abaixo.

1. (0.6 pontos) Qual é o problema do procedimento adotado por Ana?

   Resposta:

   Existem dois problemas. Primeiro, Ana não deveria conhecer a chave privada de Bruno, pois a chave privada é de conhecimento apenas de seu dono. O segundo, e mais importante, é que qualquer um tem acesso a chave pública de Bruno, pois a mesma é pública. De posse da chave pública, qualquer um pode obter K decifrando esta chave com a chave pública de Bruno. Ao obter K, qualquer um pode ler a mensagem M enviada por Ana. Repare que a mensagem M também pode ser modificada por um adversário no meio do caminho e codificada novamente utilizando K sem que Bruno saiba que a mesma foi modificada.

2. (0.6 pontos) Como você resolveria o problema? Descreva um novo procedimento criptográfico para Ana.

   Resposta:

   Ana pode resolver o problema utilizando a chave pública de Bruno K_B^+, que é de conhecimento de todos, para cifrar a chave simétrica K no passo 3 acima. Desta forma, apenas Bruno, de posse de sua chave privada, irá conseguir decifrar o resultado do passo 3 e obter a chave simétrica K que deve ser utilizada para decifrar M.