Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

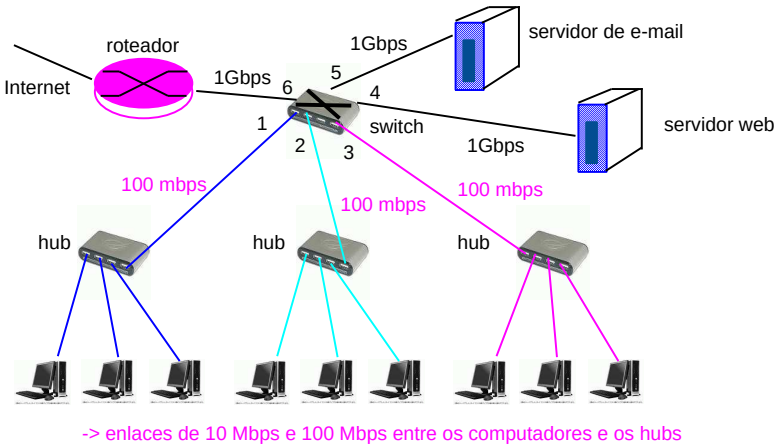
Curso de Tecnologia em Sistemas de Computação

Disciplina: Redes de Computadores II

Gabarito da AD2 - 2° semestre de 2011

Rede de interconexão [1.3 pontos]

1. **[1 ponto]** Considere a figura abaixo como sendo a rede de uma instituição.



(a) **[0.3 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: Caso 1: 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.

(b) **[0.3 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.

(c) **[0.4 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 switch 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.

2. **[0.3 pontos]** 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

Redes sem fio [2.2 pontos]

1. **[0.35 pontos]** 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. **[0.20 pontos]** Explique o que é o problema do terminal oculto em uma rede sem fio.

Resposta:

É quando um terminal não recebe o sinal do outro pois existe um obstáculo entre eles.

3. **[0.35 pontos]** Indique duas razões para que o mecanismo de acesso ao meio com detecção de colisão (CSMA/CD) não seja usado pelo protocolo para acesso sem fio IEEE802.11.

   Resposta:

   1 - O sinal enviado por um terminal A poderia colidir um sinal enviado por um terminal B e eles poderiam não detectar a colisão se um estivesse *oculto* para o outro (por exemplo devido a um obstáculo entre os dois).

   2 - Seria muito custoso um terminal que fosse capaz de enviar e receber um sinal ao mesmo tempo.

4. **[0.35 pontos]** Indique uma vantagem e uma desvantagem do uso das mensagens de reserva **CTS** e **RTS** pelo protoloco de acesso IEEE802.11.

   Resposta:

   Uma vantagem é que quando as mensagens de reserva são menores que as mensagens de dados, o tempo de colisão é menor, o que aumenta o tempo que o canal transmite informação útil (melhora o desempenho do protocolo). Uma desvantagem é o overhead causado pelo envio das mensagens.

5. **[0.25 pontos]** Dê exemplo de duas técnicas para compartilhar o meio de transmissão usadas em redes celulares e explique resumidamente como funcionam.

   Resposta:

   Combinação de FDMA/TDMA: Divisão do espectro em faixas de frequência e cada faixa de frequência é dividida em slots de tempo. Para cada terminal é alocada uma faixa de frequência e um slot de tempo.

   CDMA: Multiplexação por divisão de código. Todos os terminais transmitem ao mesmo tempo, cada um usando um determinado código.

6. **[0.35 pontos]** Quais são as principais características definidas para as redes celulares das gerações 2.5G e 3G ?

   Resposta:

   Geração 2.5G: permite transmissão de voz e dados com velocidade da ordem de centenas de kilobits por segundo.

   Geração 3G: permite transmissão de dados e voz com velocidade da ordem de 2Mbps para distâncias indoor e entre 144Kbps e 384Kbps para distâncias maiores e usuário móveis.

7. **[0.35 pontos]** Em uma rede CDMA onde N estações tem dados para transmitir como é feita a codificação do sinal no emissor dos dados e a decodificação do sinal no receptor ?

   Resposta:

   Codificação no emissor : O bit de dados a ser transmitido é *multiplicado* pelo código atribuído ao emissor. Desta forma se o código possui 8 bits, para cada bit de dados gerado, serão transmitidos 8 bits.

   Canal de dados : Dado que cada uma das N estacões gerou uma sequência de 8 bits, estas N sequências são *somadas* e transmitidas pelo canal, gerando um vetor v_m, $m = 1, 8$.

Decodificação no receptor : O receptor faz o produto interno do vetor v_m recebido com o código do emissor (c_m), soma os elementos do produto interno e divide pelo número de bits do código (M) para obter o bit de dados enviado. A operação realizada pelo receptor está representada na equação abaixo:

$bit\_recebido = \sum_{m=1}^{M} v_m * c_m/M$

onde M é o número de bits do código usado pelo emissor.

Aplicações Multimídia [3.0 pontos]

1. **[0.3 pontos]** Descreva as principais diferenças entre o conteúdo de aplicativos convencionais (ex. email) e aplicativos multimídia (ex. voz-sobre-IP)?

   Resposta:

   Aplicativos convencionais geralmente não toleram perdas de pacotes e necessitam de confiabilidade na transmissão dos dados. Entretanto, aplicativos multimídia geralmente toleram perdas de pacotes, funcionando de forma satisfatória mesmo quando não há confiabilidade. Por outro lado, aplicativos convencionais geralmente toleram atrasos inseridos pela rede, inclusive variância no atraso. Entretanto, aplicativos multimídia geralmente não toleram atrasos na rede, podendo comprometer o uso do aplicativo.

2. **[0.3 pontos]** Enumere as três classes de aplicativos multimídia e descreva as principais caracterísitcas de cada classe. Dê ao menos um exemplo de aplicativo que você conheça de cada classe.

   Resposta:

   As três classes são: 1) aplicativos streaming de vídeo armazenado; 2) aplicativos streaming em tempo real; 3) aplicativos multimídia interativos. Respectivos exemplos de aplicativos são: YouTube, a rádio CBN na Internet, e o Skype.

3. **[0.3 pontos]** Defina o que significa "streaming". Por que aplicativos multimídia utilizam esta técnica?

   Resposta:

   Streaming significa iniciar o consumo dos dados antes do término da transmissão. Aplicativos multimídia utilizam esta técnica para reduzir o tempo que os usuários precisam aguardar antes de inciarem a consumir o conteúdo (ex. assistir a um vídeo). Pois o conteúdo começa a ser consumido pelo aplicativo (e usuário) antes de ser transmitido por completo.

4. **[0.3 pontos]** Defina o que é "atraso fim-a-fim"e "jitter". Qual é a diferença entre estas medidas?

   Resposta:

   Atraso fim-a-fim é o tempo que leva um pacote desde o instante que ele sai da sua origem até o instante em que ele chega ao seu destino. O jitter é o tempo desde a chegada de um pacote até o instante de chegada do próximo pacote, ou seja, o tempo entre a chegada de dois pacotes consecutivos. O primeiro mede o tempo que leva o pacote para ir da origem ao destino, e o segundo mede o tempo entre a chegada de dois pacotes.

5. **[0.3 pontos]** Qual é o tipo de serviço oferecido pela Internet de hoje? Que tipo de garantias este serviço oferece aos aplicativos?

   Resposta:

Serviço oferecido hoje pela Internet: *Best Effort* ou Melhor Esforço. Este serviço não oferece nenhuma garantia relacionada ao atraso aos aplicativos, tal como o atraso máximo dos pacotes ou a taxa de transmissão mínima.

6. **[0.3 pontos]** Explique como aplicativos multimídia lidam com usuários que possuem diferentes restrições de largura de banda (ou seja, com diferentes taxas de acesso à rede)?

   Resposta:

   Para lidar com este problema, aplicativos multimídia codificam a mídia (ex., vídeo ou áudio) com diferentes taxas de compressão, afetando diretamente a qualidade da mídia, mas permitindo que usuários com largura de banda distintas tenham acesso ao mesmo. Por exemplo, um vídeo pode estar codificado a 100Kbps e também a 500Kbps, de forma que usuários que tenham banda larga de 200Kbps e 1Mbps possam assistir ao vídeo, mas com diferentes qualidades.

7. **[0.3 pontos]** Explique para que serve e como funciona a técnica de "bufferização do no cliente".

   Resposta:

   A técnica serve para reduzir a variância do atraso dos pacotes introduzido pela rede. Com a bufferização, o aplicativo consome os dados do buffer na taxa necessária, reduzindo a chance de um pacote não estar presente no cliente no instante em que o mesmo precisa ser consumido. A técnica funciona da seguinte maneira: os pacotes são inicialmente armazenados em um buffer até que um número suficiente de pacotes tenha sido recebido. Somente então o aplicativo inicia o consumo dos pacotes do buffer.

8. **[0.3 pontos]** Explique para que serve e como funciona o mecanismo de FEC visto em aula.

   Resposta:

   O mecanismo de FEC serve para recuperar pacotes que foram descartados pela rede sem a necessidade de retransmiti-los. Os pacotes de dados originais são agrupados em blocos, por exemplo em blocos de 3 pacotes. O FEC é um novo pacote obtido através dos pacotes que formam o bloco e enviado juntamente com os pacotes originais, no final do bloco. O FEC é obtido fazendo o XOR (operação binária) dos bits referentes aos pacotes de um mesmo bloco. Se um pacote for perdido no bloco, podemos utilizar o pacote FEC e os demais pacotes do bloco para recuperar o pacote perdido. Basicamente, ao fazermos o XOR destes pacotes com o FEC, recuperamos o pacote perdido. O overhead deste algoritmo é de 1 pacote a cada n, onde n é o número de pacotes do bloco. Neste exemplo, o overhead é de 1 em 3.

9. **[0.3 pontos]** Explique as desvantagens de usarmos retransmissão de pacotes perdidos em aplicativos multimídia.

   Resposta:

   O uso de retransmissão para recuperar pacotes perdidos, em geral requer detectar a perda, solicitar uma retransmissão, e aguardar pela chegada do pacote retransmitido. Este processo é geralmente muito demorado para aplicativos de tempo real, que possuem pouca flexibilidade de tempo. Devido a estes longos atrasos, mecanismos de retransmissão podem afetar a interatividade do usuário.

10. **[0.3 pontos]** Explique para que serve e como funciona o mecanismo de *interleaving* de pacotes visto em aula.

Resposta:

A técnica de interleaving serve para espalhar as perdas de blocos pela sequência de blocos sendo transmitida. Para fazer o interleaving nos dados a serem transmitidos, definimos um tamanho de bloco, B e um número de blocos por pacote, K. Os pacotes a serem transmitidos irão conter K blocos de informação cada um de tamanho B. Entretanto, os dados não serão transmitidos na ordem em que são gerados. Em particular, cada pacote a ser transmitido contém blocos de todos os outros pacotes originais. Por exemplo, o primeiro pacote a ser transmitido contém o primeiro bloco de todos os pacotes originais, o segundo pacote contém o segundo bloco de todos os pacotes originais, e assim sucessivamente. Desta forma, se um pacote for perdido, teremos uma perda de blocos espalhada. A qualidade do conteúdo recebido é superior neste caso, apesar da mesma quantidade de informação ser perdida.

Segurança em Redes [3.5 pontos]

1. **[0.35 pontos]** Segurança em redes é geralmente obtida quando a comunicação entre duas entidades possui a garantia de certas propriedades. Quais são estas propriedades?

   Resposta:

   Segurança em redes é obtida quando uma ou mais das seguintes propriedades é garantida pelo protocolo de comunicação: autenticidade, integridade, responsabilidade (saber que o transmissor realmente enviou a mensagem) e disponibilidade.

2. **[0.35 pontos]** Qual é a diferença entre autenticidade e integridade? É possível ter uma propriedade sem ter a outra? Justifique sua resposta.

   Resposta:

   Autenticidade é a propriedade que garante que uma determinada entidade conhece a identidade da outra entidade com a qual ela está se comunicando. Integridade garante que a informação não é alterada durante sua transmissão. Sim, é possível ter autenticidade sem integridade. Por exemplo, podemos autenticar uma entidade antes de iniciar a comunicação, entretanto, a comunicação pode não ter integridade, sendo possível que os dados sejam alterados durante a comunicação.

3. **[0.35 pontos]** Descreva como funciona criptografia com chave pública/privada. Dê um exemplo de como Ana pode enviar uma mensagem confidencial a Bruno utilizando esta técnica.

   Resposta:

   Criptografia com chave pública/privada utiliza um par de chaves: uma pública, que é de conhecimento de todos; e outra privada, que é de conhecimento apenas da entidade que gerou o do par de chaves. Uma mensagem cifrada com a chave pública só pode ser decifrada com a respectiva chave privada. Desta forma, para enviar uma mensagem cifrada, o transmissor deve utilizar a chave pública do receptor para cifrar a mensagem. O receptor, e somente ele, possui a chave privada capaz de decifrar a mensagem.

   Ana pode enviar uma mensagem confidencial M a Bruno, cifrando esta mensagem com a chave pública de Bruno, K_B^+, que é de conhecimento de todos. Desta forma, apenas Bruno pode decifrar a mensagem $K_B^+(M)$ enviada por Ana, pois apenas Bruno tem a chave privada K_B^-.

4. **[0.35 pontos]** Utilizando a cifra da substituição apresentada em aula (ver slides), cifre o texto "uma coisa trivial" e decifre o texto "ky cjumk shlkiistcg".

Resposta:

Ver slide 9 da aula 19

5. **[0.35 pontos]** O que é, e para que serve o DES?

   Resposta:

   O DES é um algoritmo de criptografia baseado em chave simétrica. Este algoritmo serve para garantir a confidencialidade da comunicação entre duas entidades, uma vez que o algoritmo é utilizado para cifrar e decifrar mensagens.

6. **[0.35 pontos]** Descreva como funciona o "ataque do homem-no-meio" durante o procedimento de autenticação com chave pública/privada. Como podemos nos defender contra este tipo de ataque?

   Resposta:

   Neste ataque, o adversário intercepta a comunicação entre as duas entidades que querem se comunicar de forma segura. O adversário finge ser a entidade com a qual a outra entidade quer ser comunicar da seguinte forma. O adversário envia uma chave publica que não corresponde a chave publica da outra entidade (ver detalhes no livro texto). A outra entidade não sabe disto, e utiliza esta chave pública para cifrar os dados. A chave privada correspondente é de conhecimento do adversário, que a utiliza para decifrar as mensagens. Para se defender deste ataque, as duas entidades que querem sem comunicar devem conhecer a priori a chave pública da outra. Ou então ser capaz de verificar que a chave pública que recebem é realmente a chave pública da outra entidade.

7. **[0.35 pontos]** Explique o que é *message digest* (resumo de mensagem) e para que ele serve? Explique o que é MD5.

   Resposta: O *message digest* (resumo de mensagem), como o nome já diz, é um resumo de uma mensagem M gerado a partir de alguma função criptográfica (algoritmo). O message digest serve para garantir a integridade da mensagem M durante sua transmissão. Ou seja, uma mensagem M deve ser enviada juntamente com seu resumo $H(M)$, para detectar se a mesma foi modificada durante sua transmissão.

   O MD5 é um algoritmo para gerar MAC (Message Autentication Code), conhecido também como *digest* (ou resumo). Tais resumos são utilizados para garantir a integridade da mensagem sendo transmitida, uma vez que qualquer mudança nos bits da mensagem irá levar a uma mudança em seu resumo.

8. **[0.35 pontos]** Descreva como funciona o conceito de "assinatura digital". Quais são as propriedades que este mecanismo oferece?

   Resposta:

   Assinatura digital tenta espelhar as propriedades da assinatura que conhecemos no mundo real. A assinatura digital serve para garantir que um determinado documento foi composto ou avalizado por alguém ou alguma entidade. A assinatura digital é verificável e não pode ser forjada. A segurança de uma assinatura digital pode ser até maior do que no mudo real. Ver mais detalhes no livro texto!

9. **[0.35 pontos]** Descreva de forma sucinta o funcionamento de um firewall baseado em filtro de pacotes. De um exemplo de regra.

   Resposta:

   Um firewall baseado em pacotes inspeciona cada pacote que chega ao firewall para determinar se o pacote deve ou não ser encaminhado. Esta decisão é feita com base

em regras que foram estipuladas e estão armazenadas no firewall (colocadas lá pelo administrador da rede). As regras são baseadas no conteúdo do cabeçalho dos pacotes e podem ser usadas para permitir ou proibir que o pacote seja encaminhado. Por exemplo, uma regra pode estipular que todo o tráfego cujo IP de destino pertença ao prefixo 146.164.0/24 seja bloqueado.

10. [**0.35 pontos**] Descreva como você pode obter a senha de um usuário que acessa um Website protegido por senha. Como você se defenderia do seu ataque?

    Resposta:

    Se tivermos acesso a rede local onde fica o servidor Web, poderíamos capturar os pacotes que passam pela rede (com o tcpdump, por exemplo) e descobrir a senha utilizada pelo usuário. Para se defender, precisamos garantir que nenhum computador intruso terá acesso a rede local do servidor Web. Outra idéia é utilizar um protocolo mais seguro, como o HTTPS, que utiliza criptografia fim-a-fim, negociando uma chave simétrica antes de iniciar a comunicação. Desta forma, a senha do nosso usuário não será enviada em texto simples.