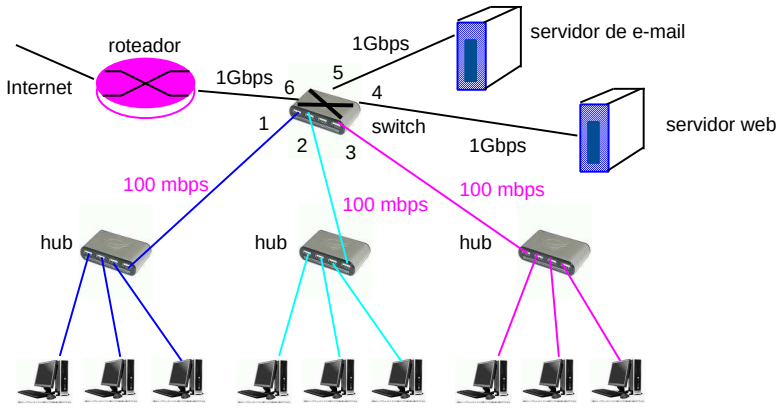
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AD2 - 1° semestre de 2008

1. **[3 pontos]** Considere a figura abaixo como sendo a rede de uma instituição.



(a) **[1 ponto]** 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) **[1 ponto]** 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) **[1 ponto]** 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.

2. **[1 ponto]** 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

3. **[1 ponto]** 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.

4. **[1 ponto]** 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.

5. **[1 ponto]** 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.

6. **[1 ponto]** 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.

7. **[1 ponto]** 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.

8. **[1 ponto]** 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.

9. **[1 ponto]** O que caracteriza os aplicativos multimídia?

   Resposta:

   O fato de lidarem com *mídia contínua* é a principal característica de aplicativos multimídia. Mídia contínua se refere ao tipo de dados utilizado por este aplicativo, que possui uma forte dependência temporal.

10. **[1 ponto]** Quais são as principais diferenças entre os aplicativos convencionais (como email) e os aplicativos multimídia (como Skype)?

    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.

11. **[1 ponto]** 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 aos aplicativos, tal como o atraso máximo dos pacotes ou a taxa de transmissão mínima.

12. **[1 ponto]** 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.

13. **[1 ponto]** Porque aplicações interativas de tempo real (como o Skype) estão mais suscetíveis a perda de qualidade do que aplicações de streaming de conteúdo armazenado?

    Resposta:

    Por que para manter a interatividade, os aplicativos possuem uma maior restrição de tempo. Ou seja, os aplicativos tem menos tempo para lidar com os dados, não podendo aguardar por muito tempo antes de iniciar o consumo do conteúdo. Em aplicativos de streaming, as restrições temporais são geralmente mais flexíveis.

14. **[1 ponto]** 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.

15. **[1 ponto]** 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.

16. **[1 ponto]** 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.

17. **[1 ponto]** Descreva como funciona criptografia com chave pública/privada.

    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.

18. **[1 ponto]** Utilizando a cifra da substituição apresentada em aula (ver slides), cifre o texto "uma coisa e trivial"e decifre o texto "ky cjumk shlkiistcg".

    Ver slide 9 da aula 19!

19. **[1 ponto]** 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.

20. **[1 ponto]** Descreva como funciona o "Ataque do homen-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.

21. **[1 ponto]** O que é, e para que serve o MD5?

    Resposta:

    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 mundança em seu resumo.

22. **[1 ponto]** 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!

23. **[1 ponto]** Descreva como você pode obter a senha de um usuário que acessa um Website protegido. Como você se defenderia do seu ataque?

    Resposta:

    Se tivermos acesso a rede local onde fica o servidor Web, poderiamos 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.