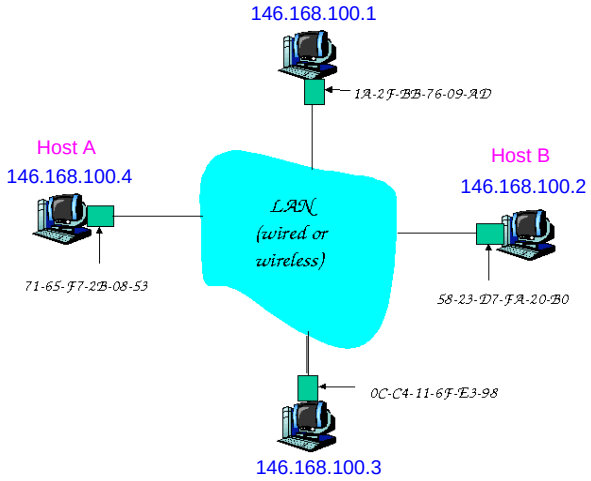
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AD2 - 2° semestre de 2008

1. **[1 ponto]** Suponha a rede da figura abaixo onde o *host A* deseja enviar uma mensagem para o *host B*. Considere que *A* não possui o endereço MAC de *B*. Descreva as mensagens do protocolo ARP para que *A* possa enviar a mensagem para *B*.



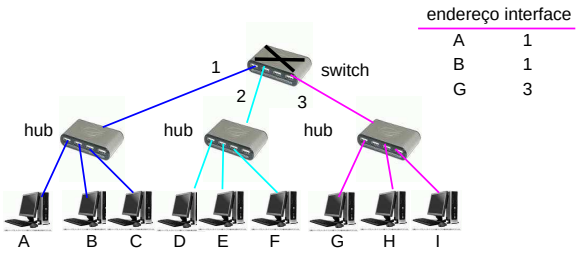
Resposta:

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.

2. **[2 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.



- (0.5) Suponha que E envie uma mensagem para G. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? Explique porque e mostre a nova tabela após a mensagem de E chegar ao switch. Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

  Resposta:

  Sim, ocorre é criada uma nova entrada que relaciona o endereço de E com a respectiva interface onde E se encontra, pois este host não constava da tabela do switch.

  A nova tabela é a seguinte:

endereço	Interface
A	1
B	1
G	3
E	2

  Ele irá consultar a sua tabela e encaminhar pela interface 3 onde está o host G.

- (0.5) Agora suponha que G envie uma mensagem (resposta) para E. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? Explique porque e mostre a nova tabela após a mensagem de G chegar ao switch. Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

  Resposta:

  Não ocorre nehuma atualização pois G já está na tabela. A tabela permanece igual a tabela mostrada no item acima. Ele irá consultar a sua tabela e encaminhar pela interface 2 onde está o host E.

- (0.5) Descreva duas vantagens de switches sobre hubs.

  Resposta:

  1 - Switches isolam tráfego. Eles encaminham seletivamente os quadros consultando a sua tabela de encaminhamento. As tabelas são atualizadas através de um algoritmo de aprendizado.

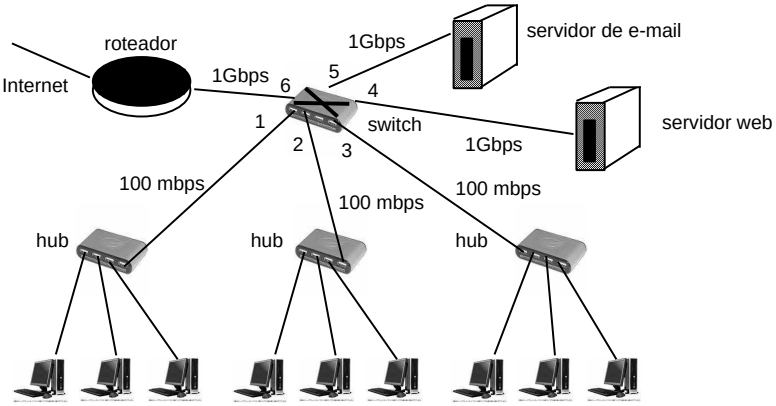
  2 - É possível interconectar segmentos de rede de velocidades diferentes pois switches possuem buffer.

- (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:

  Este cenário ocorre quando dois hosts estão conectados ao switch através da mesma interface. Por exemplos, hosts A e B na topologia acima.

3. **[2 pontos]** Considere a figura abaixo como sendo a rede de uma instituição.



-> enlaces de 10 Mbps e 100 Mbps entre os computadores e os hubs

(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: vazão máxima agregada é de 90 Mbps. Neste caso o gargalo é a placa de rede dos computadores.

Caso 2: Todos os computadores estão conectados ao hub a 100Mbps: vazão máxima agregada é de 300 Mbps. Neste caso o gargalo é o enlace entre um hub e o switch.

(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 único domínio de colisão pois hubs não isolam o tráfego. Se tivermos switches no lugar de hubs, teríamos 3 domínios de colisão.

4. **[1 ponto]** 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:

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

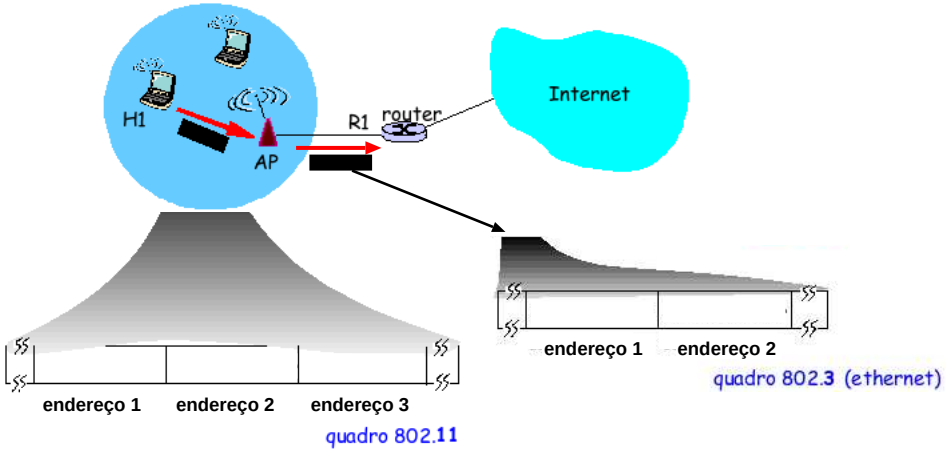
onde M é o número de bits do código usado pelo emissor.

5. **[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.

6. **[1 ponto]** Considere a topologia da figura abaixo, onde um *host H1* está enviando uma mensagem que deve ser roteada pelo roteador *R1*. *H1* está em uma rede IEEE802.11 infra-estruturada e o AP (ponto de acesso) desta rede, está ligado a Internet através do roteador *R1*.



   (a) (0.5) Descreva quais endereços devem estar contidos nos campos *endereço 1,2 e 3* do quadro 802.11 e nos campos *endereço 1 e 2* do quadro ethernet. (Por exemplo, endereço MAC do AP.)

   Resposta:

   Quadro 802.11:

   Endereço 1: endereco MAC do AP (estacão de destino).

   Endereço 2: endereco MAC de H1 (estacão de origem).

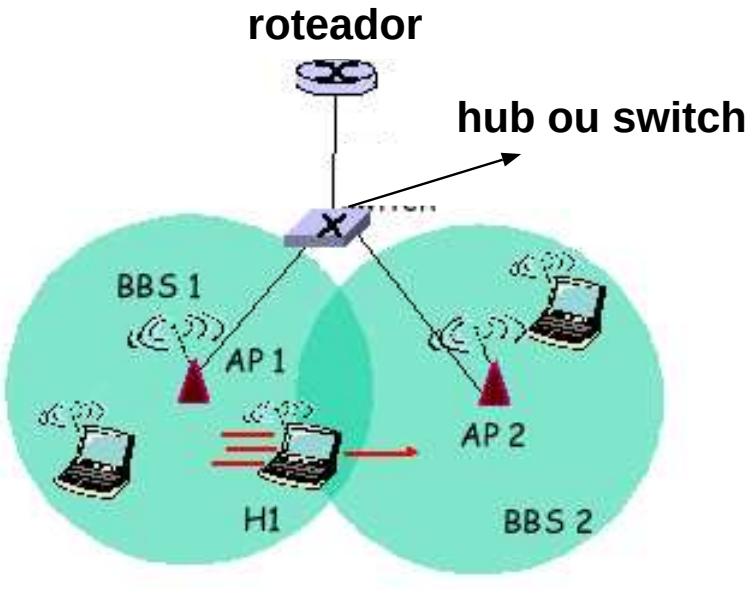
   Endereço 3: endereco MAC do roteador que está conectando a sub-rede da BSS a outras sub-redes. Na figura acima é o endereco MAC do roteador R1.

   Quadro ethernet:

   Endereço 1: endereco MAC de R1 (estacão de destino).

   Endereço 2: endereco MAC de H1 (estacão de origem).

(b) Suponha que o host *H1* se desloque e passe a ser atendido por um outro AP conforme a figura abaixo. Considerando que a interconexão é feita usando um hub, o deslocamento de *H1* interfere no funcionamento do hub ? (Explique porquê).



Resposta:
Não, pois o hub não possui tabela de encaminhamento e portanto não faz encaminhamento seletivo dos quadros para as sub-redes adequadas.

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]** 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.

9. **[1 ponto]** 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.

10. **[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 relacionada ao atraso aos aplicativos, tal como o atraso máximo dos pacotes ou a taxa de transmissão mínima.

11. **[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.

12. **[1 ponto]** Defina o que é "atraso fim-a-fim"e "jitter". Qual é a diferença entre estas medidas?

    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.

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 *interleaving* de pacotes visto em aula.

    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.

16. **[1 ponto]** 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.

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 trivial"e decifre o texto "ky cjumk shlkiistcg".

    Resposta:

    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 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.