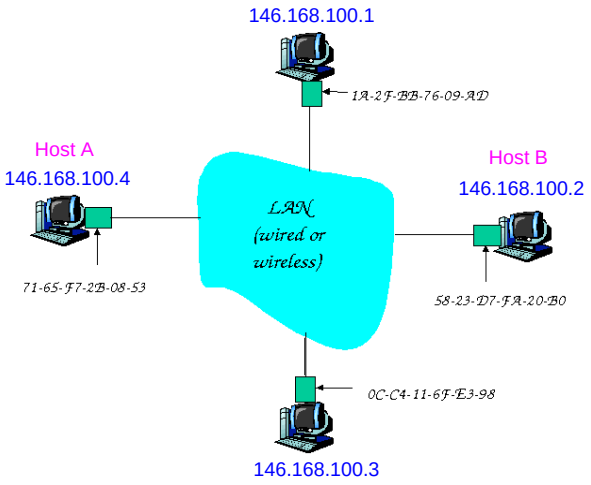
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AD2 - 2° semestre de 2007

1. **[1.2 pontos]** 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*.



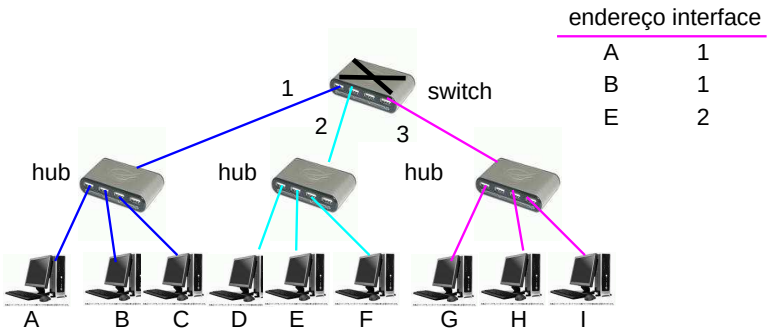
Resposta:

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. **[1.8 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.



- (0.6) Suponha que E envie uma mensagem para G. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? (Explique porque). Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

  Resposta:

  Não ocorre atualização pois o switch já possui uma entrada na sua tabela que mapeia o endereço de E com a respectiva interface onde E se encontra.

  Ele irá encaminhar pelas interfaces 1 e 3 pois não possui uma entrada na sua tabela para o host G. Ele usa neste caso o algorimo de *flooding*.

- (0.6) Agora suponha que G envie uma mensagem (resposta) para E. Quando a mensagem chega no switch ocorre alguma atualização na sua tabela ? (Explique porque). Por quais interfaces o switch irá encaminhar a mensagem ? (Explique porque).

  Resposta:

  Sim, pois o switch irá criar uma entrada que mapeia o endereço de G na interface 3 que é onde G se encontra.

  Ele irá encaminhar pela interface 2 após cunsulta à sua tabela que indica onde E se encontra.

- (0.6) 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.

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]** 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]** Descreva dois motivos para que o protocolo CSMA/CD não seja usado em uma rede sem fio.

   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]** O padrão IEEE802.11 tem dois modos de operação: com e sem reserva. 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 médio 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.

7. **[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 precisam de uma comunicação confiável, sem que haja perda de informação durante a transmissão dos dados. Entretanto, eles podem

tolerar atrasos aleatórios introduzidos pela rede durante esta transmissão. Aplicativos multimídia geralmente possuem o requerimento inverso. Ou seja, não precisam de uma comunicação totalmente confiável, sendo tolerantes a perda de informação, entretanto não toleram muito bem atrasos durante a transmissão, principalmente variações do atraso.

8. **[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.

9. **[1 ponto]** Defina o que é "atraso fim-a-fim"e "jitter". Qual é a diferença entre estas medidas?

   Resposta:

   Atraso fim-a-fim é o intervalo de tempo desde o instante em que um pacote é enviado pelo transmissor até o instante em que o mesmo pacote é recebido pelo receptor. O jitter é a variação dos atrasos fim-a-fim, quando consideramos diversos pacotes de uma mesma conexão. O atraso fim-a-fim diz respeito a um único pacote (e cada pacote possui um atraso fim-a-fim). O jitter mede a variação deste atraso, ou seja, o quanto o atraso varia de um pacote para outro. Um jitter pequeno quer dizer que o atraso não varia muito, mas não quer dizer que não temos atraso.

10. **[1 ponto]** Por que aplicativos multimídia utilizam a técnica de "buferização no cliente"?

    Resposta:

    Para melhorar a qualidade do vídeo ou do áudio que é recebido pelo cliente. Esta é uma das técnicas empregadas pelos aplicativos para lidarem com a falta de garantias do serviço oferecido pela Internet de hoje. Esta técnica tem como objetivo reduzir o jitter dos pacotes para a aplicação.

11. **[1 ponto]** Descreva como funciona o esquema FEC de redundância apresentado em aula. Qual é o *overhead* (aumento relativo do número de bytes transferidos) deste esquema?

    Resposta:

    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.

12. **[1 ponto]** Por que empresas que disponibilizam conteúdo multimídia na Internet (como vídeo) geralmente oferecem o mesmo conteúdo codificado em diferentes formatos e com diferentes qualidades (isto é, diferente taxas de codificação)?

    Resposta:

    Para atender a clientes com diferentes conexões à Internet. Um cliente que possui um canal de acesso banda larga possui maior largura de banda, e por isto pode assistir a

um conteúdo com melhor qualidade, codificado com uma taxa maior. Entretanto, um cliente que se conecta via acesso discado, por não ter banda suficiente, não pode assistir o conteúdo neste formato. Porém este cliente pode assistir ao mesmo conteúdo com uma qualidade mais baixa. Logo, para atender a uma variedade maior de clientes, o provedor do conteúdo disponibiliza o mesmo conteúdo em múltiplos formatos e taxas de codificação.

13. **[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:

    As principais propriedades para garantir a segurança em redes são: Confidencialidade: somente o transmissor e o respectivo receptor conseguem ler a mensagem; Autenticação: receptor quer confirmar identidade do transmissor (e vice-versa); Integridade: transmissor e receptor não querem que mensagem seja alterada sem que isto possa ser detectado; Acesso e disponibilidade: serviços de rede devem estar sempre acessíveis e disponível aos usuários.

14. **[1 ponto]** Qual é a diferença entre confidencialidade e integridade? É possível ter uma propriedade sem ter a outra? Justifique sua resposta.

    Resposta:

    Confidencialidade garante que uma terceira pessoa não terá acesso ao conteúdo da informação sendo transmitida. Integridade garante que a informação não é alterada durante sua transmissão. Sim, é possível ter integridade sem confidencialidade. Por exemplo, podemos proteger uma mensagem para que a mesma não possa ser modificada (via hash e criptografia, por exemplo) sem ter que "esconder"seu conteúdo.

15. **[1 ponto]** Utilizando a cifra da substituição apresentada em aula (ver slides), cifre o texto "voce nao pode ler"e decifre o texto "jmvm c ichloc iczyok".

    Resposta:

    Ver slide 9 da aula 19! Dica da mensagem cifrada: "nada e se..."

16. **[1 ponto]** Descreva como funciona o "Ataque de Playback"durante o procedimento de autenticação. Como podemos nos defender contra este tipo de ataque?

    Resposta:

    O ataque consiste em repetir um determinado padrão de troca de mensagens. Ou seja, após escutar uma autenticação bem sucedida, o intruso tenta se autenticar utilizando os mesmos pacotes. Para defender deste ataque podemos usar um "nonce", que é um número aleatório gerado pela entidade que deseja autenticar a outra. Ao usarmos um nonce no processo de autenticação, o ataque de playback não irá funcionar, pois os pacotes de autenticação dependem do nonce escolhido pela parte autenticadora.

17. **[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!

18. **[1 ponto]** Descreva de forma sucinta o funcionamento de um firewall baseado em filtro de pacotes. De um exemplo de regra.

    Resposta:

    Um firewall é um software que roda no roteador de entrada/saída (gateway) de uma rede. Seu objetivo é isolar uma rede de uma determinada organização de uma outra rede qualquer, como por exemplo, a Internet pública. Isto é feito permitindo ou não que pacotes gerados de um lado da rede (interna ou externa) sejam encaminhados para o outro lado da rede (interna ou externa). Um conjunto de regras baseadas na informação contida nos pacotes (ex. protocolo, porta, etc) determina quais pacotes devem ou não ser encaminhados pelo gateway. Um exemplo de regra: descartar todos os pacotes vindos da rede externa que sejam do protocolo UDP.

19. **[1 ponto]** O que é "IP Spoofing"? Como isto pode ser utilizado?

    Resposta:

    IP Spoofing é uma técnica que consiste em mudar o endereço IP de origem de um pacote para algum endereço diferente do endereço IP da estação transmitindo o pacote. Ou seja, um computador com endereço IP x cria e transmite um pacote com endereço IP y, dando a entender que o pacote foi criado pelo computador com IP y. Existem diversas maneiras maliciosas de utilizarmos esta técnica, entre elas, enganar um máquina que recebe um pacote "spoofed"(com endereço IP forjado) que uma mensagem foi criada e transmitida por uma máquina inocente com IP y.