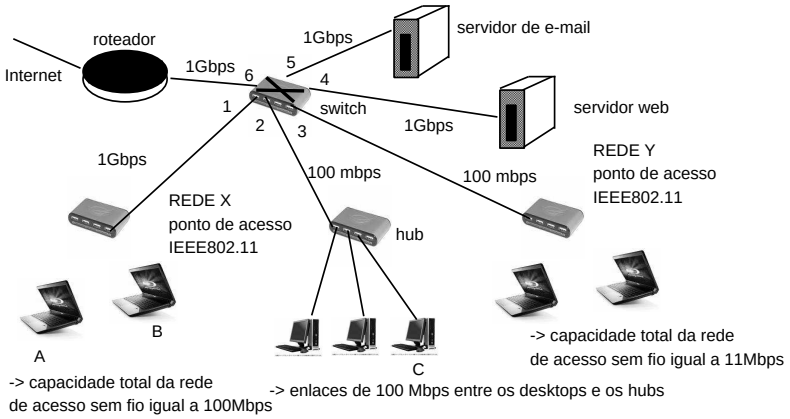
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 2° semestre de 2011

1ª questão (2.7 pontos)

Considere a figura abaixo como sendo a rede de uma instituição. Suponha que existam dois pontos de acesso sem fio IEEE802.11 para conexão de laptops. A rede sem fio X possui capacidade máxima de 100Mbps (a ser compartilhada entre os terminais sem fio) e a rede sem fio Y possui capacidade máxima de 11Mbps (a ser compartilhada entre os terminais sem fio), conforme mostrado na figura.



1. (0.5) Suponha que a rede X tenha 3 terminais conectados e a rede Y tenha 5 terminais conectados. Qual a vazão máxima de cada um dos terminais na rede X e na rede Y ?

   Resposta:

   A vazão de cada um dos terminais na rede X é de 33.33 Mbps e a vazão de cada terminal na rede Y é de 2.2 Mbps.

2. (0.5) Explique por que não é eficiente usar um protocolo com detecção de colisão (tipo CSMA/CD) em uma rede sem fio.

   Resposta:

   1 - Porque o terminal teria que enviar e receber o sinal ao mesmo tempo o que pode ser muito custoso.

   2 - Porque um terminal A poderia não detectar uma colisão com um terminal B mesmo que ela existisse, pois o terminal B poderia estar escondido para A.

3. O padrão IEEE802.11 tem dois modos de operação: com e sem reserva. Suponha que os quadros de reserva sejam iguais a 100Bytes e que a sua aplicação gere pacotes com tamanho igual a 500Kbytes. Suponha os dois cenários abaixo.

(a) (0.5) Transmissão do quadro com sucesso. Qual o overhead do protocolo nos dois casos: operação com reserva e sem reserva ? Considere a seguinte definição de overhead: *quantidade de dados transmitidos que não serão úteis para o usuário (ex: mensagens de controle) dividido pelo total dos dados transmitidos.*

Resposta:

Caso de operação com reserva: O protocolo envia duas mensagens de reserva (RTS e CTS), cada uma de 100Kbytes. Logo o overhead é igual $200/700 = 0.28$

Caso de operação sem reserva: Não existem mensagens de controle, portanto o overhead é zero.

(b) (0.5) Transmissão do quadro sem sucesso (colisão). Neste cenário, qual o modo de operação seria mais eficiente: com ou sem reserva ? Explique porquê.

Resposta:

No caso de colisão, dado que o quadro de reserva é bem menor que o quadro de dados, a operação com reserva é mais eficiente pois o meio de transmissão ficará ocupado transmitindo informação inútil durante um tempo menor (tempo de transmissão do quadro de reserva de 100 Kbytes). Na operação sem reserva o meio ficará ocupado durante um tempo maior (tempo de transmissão de um quadro de 500 Kbytes).

4. (0.7) Suponha que o computador A queira enviar uma mensagem ao computador C mas não possua o endereço MAC de C. Que protocolo deve ser usado para que A obtenha o endereço MAC de C ? Descreva as mensagens que devem ser trocadas entre A e C até que A obtenha o MAC de C.

   Resposta:

   O protocolo é o ARP. As mensagens são as descritas abaixo.

   Passo 1: A envia pacote ARP query em broadcast contendo endereço IP do roteador pois descobre através da sua tabela de roteamento IP que C não está na mesma rede local que ele, portanto deve encaminhar a mensagem para o roteador.

   Passo 2: O roteador recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de A.

   Passo 3: A recebe o pacote do roteador e atualiza a sua tabela ARP criando uma entrada com o endereço IP do roteador e o respectivo MAC. A envia quadro cujo endereco MAC de destino é o MAC do roteador. Neste quadro, A encapsula o pacote destinado a C (IP destino é C).

   Passo 4: Quando o roteador receber o quadro enviado por A, ele usará o IP destino de C para descobrir por qual interface deve encaminhá-lo.

2ª questão (2.3 pontos)

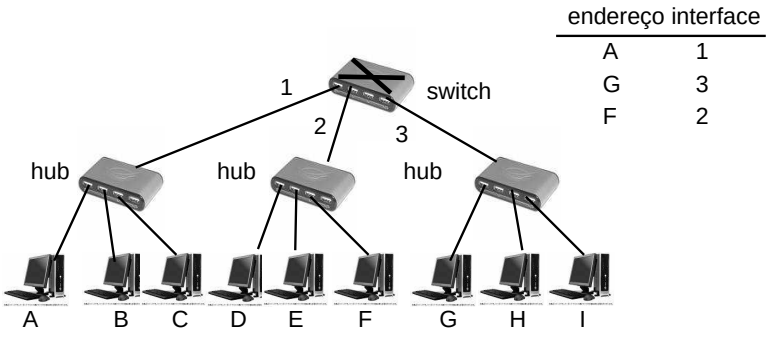
Interconexão de redes

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 B* destinada ao *host F* será encaminhada ? (Explique porquê.)

   Resposta:

   Será encaminhada pela interface 2 pois o host F está na tabela do switch.



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
F	2
B	1

3. (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:

   No caso dos dois hosts (origem e destino da mensagem) estarem na mesma rede local.

4. (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.

5. (0.3) Cite uma vantagem de switches em relação a hubs.

   Resposta:

   Switches isolam domínios de colisão.

$3^{\underline{a}}$ questão (2.5 pontos)

Aplicações Multimídia. Considere o tipo de serviço oferecido pela Internet de hoje, conhecido como *best effort* e responda às perguntas abaixo.

1. (0.6) Cite algumas razões para a Internet oferecer apenas o serviço *best effort* a seus aplicativos.

   Resposta: Podemos citar diversas razões pela qual a Internet oferece apenas o serviço *best effort* a seus aplicativos, tais como:

- Manter a simplicidade dos equipamentos que definem a rede, como roteadores, switches e gateways.
- Manter a simplicidade dos protocolos que operam a rede, tais como protocolos da camada de rede (IP) e de transporte (UDP e TCP).
- Não impor restrições aos dispositivos que desejam se conectar a rede, como por exemplo restrições mínimas de banda ou restrições de processsamento mínino.
- Não demandar a implementação de protocolos específicos nas camadas de enlace e aos aplicativos.
- Manter um baixo custo de conexão à rede, uma vez que qualquer dispositivo com quaisquer características pode se conectar.

2. (0.6) Por que este tipo de serviço, de forma geral, não é adequado para aplicativos multimídia?

   Resposta: Porque o serviço *best effort* não oferece nenhum tipo de garantia com relação a taxa de transmissão de pacotes nem com relação ao atraso fim-a-fim dos pacotes. Como aplicativos multimídia são muito sensíveis ao atraso e a variações no atraso, este serviço de forma geral não é adequado.

3. (0.7) Cite duas técnicas empregadas por aplicativos multimídia para mascarar os efeitos negativos do serviço *best effort*. Para cada técnica citada, descreva qual efeito negativo a técnica mascara.

   Resposta:
   Bufferização do lado do cliente. O objetivo desta técnica é mascarar os atrasos impostos pela rede aos pacotes dos aplicativos. Mais ainda, esta técnica serve para mascarar as variações do atraso dos pacotes, pois pequenas variações são aliviadas pelo buffer do lado do cliente.

   Protocolo UDP. Ao utilizar o protocolo de transmissão UDP, os aplicativos multimídia não estão sujeitos a variação da taxa de transmissão imposta pelo protocolo TCP, que adapta a taxa de transmissão devido ao mecanismo de controle de congestionamento. Ao utilizar o protoclo UDP, os aplicativos se tornam menos sujeitos a variações na taxa de transmissão.

   Redundância. A redundância no fluxo de dados multimídia permite a recuperação de dados perdidos, ou seja, pacotes descartados pela rede, sem que seja necessário a retransmissão dos dados. Desta forma, o aplicativo cliente pode mitigar o efeito de perda de pacotes, utilizando a redundância para recuperar alguns dos pacotes que foram descartados pela rede.

4. (0.6) Considere um grande provedor de conteúdo multimídia na Internet, como o serviço G1 da Globo. O provedor gostaria de vender acesso a vídeos em tempo real a uma variedade de clientes que possuem grandes diferenças em suas bandas de acesso (por exemplo, clientes com banda de acesso de 256Kbps, 1Mbps, 2Mbps, 5Mbps). O que o provedor pode fazer para atender de forma satisfatória todos os seus clientes?

   Resposta: O provedor poderia codificar os vídeos múltiplas vezes utilizando taxas de codificação distintas e disponibilizar estas diversas codificações para atender de forma satisfatória todos os seus clientes. Desta forma, clientes com banda de acesso menor podem assistir um vídeo em tempo real utilizando a codificação de mais baixa qualidade sem ter que esperar muito para iniciar a reprodução. Da mesma forma que clientes com banda de acesso maiores podem também assistir a um vídem em tempo real utilizando a codificação de mais alta qualidade. Desta forma, ambos podem assistir vídeos em

tempo real, com baixa latência inicial, cada um com a qualidade que seja suportada pela sua banda de acesso.

$4^{\underline{a}}$ questão (2.5 pontos)

Segurança em Redes: Responda às perguntas abaixo.

1. (0.5) Qual é á principal diferença entre criptografia com chave simétrica e criptografia com chave pública/privada?

   Resposta: A principal diferença é que em criptografia simétrica as duas partes comunicantes precisam compartilhar um segredo, que é a chave do algoritmo criptográfico. Entretanto, na criptografia com chave pública/privada as duas partes comunicantes não precisam compartilhar um segredo, sendo suficiente que uma das partes conheça a chave pública da outra, que é informação pública.

2. (0.5) Explique porque um ataque de homem-no-meio (*man-in-the-middle attack*) pode ocorrer quando utilizamos criptografia com chave pública/privada.

   Resposta: Este tipo de ataque pode ocorrer quando uma das partes comunicantes não conhece a chave pública da outra. Suponha que A não conhece a chave pública de B. Neste caso, B precisa informar sua chave pública para A, de forma que A possa enviar dados confidenciais para B. Logo, B pode transmitir sua chave pública para A. Entretanto, esta informação pode ser interceptada por uma outra entidade e trocada por uma outra chave pública. Suponha que C intercepta a chave pública de B sendo transmitida para A e troca esta chave por outra chave publica qualquer, de conhecimento de C. Neste caso, A não sabe que está usando uma chave pública que não é de B, e dados cifrados com esta chave pública serão decifrados por C.

3. (0.5) Explique para que serve um *nonce*, utilizado por exemplo no procedimento de autenticação com chave simétrica.

   Resposta: O *nonce* é um número gerado de maneira aleatória por uma das partes comunicantes para que a outra parte prove que é ela que está realmente no outro lado da comunicação. Ou seja, se B deseja se comunicar com A, então B pode gerar um *nonce* de maneira aleatória, enviar este *nonce* para A solicitando que A criptografe-o utilizando a chave simétrica compartilhada com B. A então envia o *nonce* cifrado para B que decifra-o usando o mesma chave simétrica e compara com o *nonce* enviado. Repare que somente A pode ter cifrado o *nonce* corretamente, pois somente ele conhece a chave simétrica. Por fim, como *nonce* é gerado aleatoriamente, *nonces* antigos, originais e cifrados, capturados por um adversário não serão úteis (que seria o *ataque de playback*).

Considere que Ana deseje enviar uma mensagem M para Bruno. Ana quer que a mensagem seja confidencial e então 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 sua chave privada K_A^-
4. Ana envia a Bruno o resultado das operações 2 e 3 acima.

(1.0) Existe algum problema com o procedimento criptográfico acima? Caso positivo, identifique o problema e mostre como você o resolveria. Caso negativo, argumente que o procedimento está correto.

Resposta: Sim, o procedimento acima possui um problema. Ao transmitir a chave simétrica K cifrada com sua chave privada, Ana permite que qualquer pessoa que tenha conhecimento de sua chave pública possa decifrar esta mensagem e obter a chave simétrica K. Como a chave públida de Ana é de conhecimento público, qualquer um poderá ter obter K. Ao ter acesso a K qualquer um poderia decifrar a mensagem M. Para resolver o problema, Ana deve cifrar a chave K utilizando a chave pública de Bruno. Desta forma, somente Bruno pode decifrar esta mensagem com sua chave privada e obter K. Como somente Bruno terá acesso a K, somente ele poderá decifrar a mensagem M, utilizando a chave simétrica K. Desta forma, garantimos a confidencialidade da mensagem M.