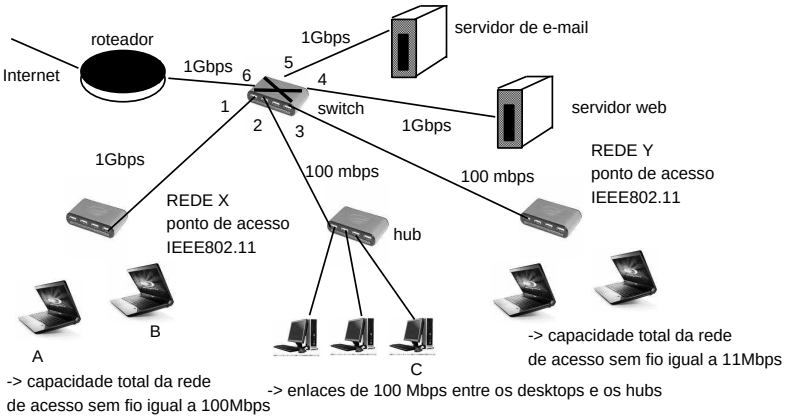
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP3 - 1° semestre de 2013

1ª questão (1.5 pontos)

Interconexão, Rede sem fio: 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 máxima de cada terminal na rede X é de $100/3 = 33.3$Mbps e na rede Y é de $11/5 = 2.2$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:

   Não é eficiente pois (i) é muito custoso para um terminal sem fio receber e transmitir um sinal ao mesmo tempo; (ii) se um terminal estiver "escondido" para o outro, a colisão não é detectada pelos terminais e os terminais podem inferir que a mensagem foi transmitida com sucesso.

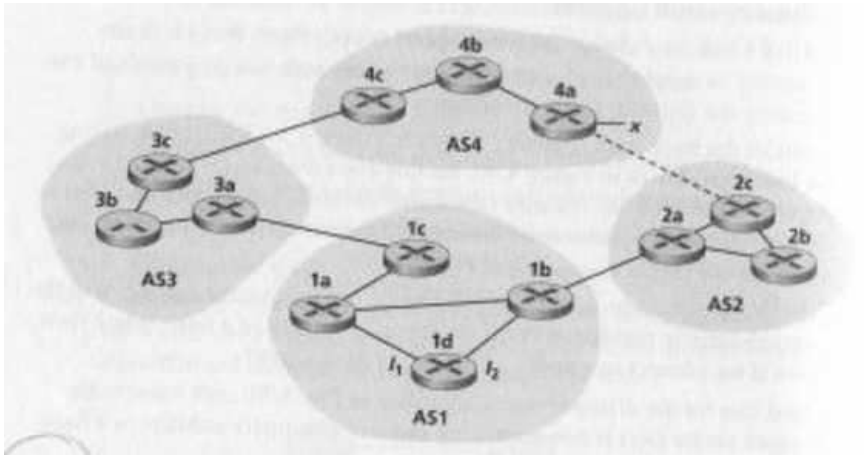
3. (0.5) Suponha que o computador A queira enviar uma mensagem ao computador C mas não possua o endereço MAC de C. Que protocolo deve ser usado para que A obtenha o endereço MAC de C ?

Resposta:

O protocolo ARP.

2$^{\underline{a}}$ questão (3.5 pontos)

Roteamento: Considere a rede da figura abaixo. Suponha que a AS3 e a AS2 estão executando o protocolo de roteamento *OSPF* e que a AS1 e a AS4 estão executando o protocolo de roteamento *RIP*. Todas as AS's estão executando o *eBGP* e o *iBGP* para comunicação entre elas. Considere que não existe conexão física entre a AS2 e a AS4 (linha pontilhada na figura).



Responda as perguntas abaixo:

1. (0.5) Através de que protocolo (OSPF, RIP, eBGP, iBGP) o roteador 4c irá conhecer o prefixo x ? Justifique.

   Resposta:

   O roteador 4c irá conhecer o prefixo x através do protocolo RIP (protocolo de roteamento usado dentro da AS4) pois o prefixo x está na mesma AS que o roteador 4c.

2. (0.5) Através de que protocolo (OSPF, RIP, eBGP, iBGP) o roteador 3c irá conhecer o prefixo x ? Justifique.

   Resposta:

   Os roteadores 3c e 4c são gateways que ligam a AS3 com a AS4, e portanto possuem uma sessão BGP externa. Como o prefixo x está na AS4, 3c irá conhecer x através do eBGP.

3. (0.5) Através de que protocolo (OSPF, RIP, eBGP, iBGP) o roteador 3a irá conhecer o prefixo x ? Justifique.

   Resposta:

   O roteador 3a está na AS3 e possui uma sessão BGP interna para que a informação de alcançcabilidade da AS4 seja divulgada dentro da AS3. Portanto irá receber a informação de alcançabilidade de x através do iBGP.

4. (0.5) Qual o caminho que um pacote irá percorrer desde a saída do roteador 1d até x ?

   Resposta:

O pacote terá que ser roteado dentro da AS1 (usando RIP), passar pela AS3 e depois AS4 pois este é o único caminho existente entre a AS1 e a AS4.

O caminho é:

Dentro da AS1: 1d, 1a, 1c (rota que possui menor número de saltos entre 1d e 1c).
Dentro da AS3: 3a, 3b, 3c (só existe essa rota entre 3a e 3c).
Dentro da AS4: 4c, 4b, 4a, x (só existe essa rota entre 4c e x).

5. (0.5) Este caminho pode mudar se existir uma conexão física entre a AS2 e a AS4 ? Justifique.

   Resposta:

   Sim, pois se existir uma conexão entre a AS2 e a AS4, existiria uma outra rota alternativa entre 1d e x que passaria pela AS1, AS2 e AS4.

6. (1.0 ponto) Cite as principais características do protocolo OSPF (ex: algoritmo usado para o roteamento, mensagens trocadas entre os nós, etc.)

   Resposta:

   Principais características do OSPF:

   (i) É um protocolo do tipo *link state* e, portanto, cada nó usa o algoritmo de Dijkstra para fazer o roteamento e o *flooding* para enviar informações a respeito dos custos/estados dos enlaces.
   (ii) Mensagens trocadas entre os nós podem ser autenticadas o que aumenta a segurança.
   (iii) Suporte a hierarquia dentro de um mesmo domínio.
   (iv) Podem ser usados múltiplos caminhos até um certo destino quando eles possuem o mesmo custo.

3^{a} questão (1.5 pontos)

Camada de Enlace: Considere uma rede local onde um enlace de comunicação está sendo compartilhado por muitas estações (usuários), por exemplo 50. Considere protocolos baseados na partição do enlace, como TDMA e FDMA, e protocolos baseados no acesso aleatório ao enlace, como o ALOHA e o CSMA. Tendo em vista as características do tráfego gerado pelos usuários, determine em que situações um tipo de protocolo será mais eficiente do que o outro. Em particular, comente sobre a vazão e o retardo observado pelos usuários em cada tipo de protocolo em função da carga de tráfego na rede. Explique sua resposta.

Resposta: Os protocolos baseados em partição do enlace, como TDMA e FDMA, são mais apropriados para situações onde há uma grande demanda pela rede, ou seja, quando todos seus usuários desejam acessar a rede simultaneamente. Neste cenário a vazão e o retardo observado pelos usuários será determinada pela divisão dos recursos do canal e não serão afetados pela alta carga na rede. Além disso, o canal será utilizado integralmente sem disperdiço de tempo, oferecendo o melhor desempenho possível. Já os protocolos baseados acesso aleatório, como o ALOHA e CSMA, são mais apropriados para situações onde há uma pequena demanda pela rede, ou seja, quando uma fração pequena de todos os seus usuários desejam acessar a rede simultaneamente. No cenário de alta demanda, a vazão e o retardo observado pelos usuários serão afetados negativamente (a vazão será baixa e o retardo alto) em função das muitas colisões que irão ocorrer, uma vez que todos os usuários querem acessar o canal simultaneamente. Devido às colisões, teremos um grande disperdício de tempo no canal e seu desempenho será muito baixo.

4ª questão (1.5 pontos)

Aplicações Multimídia: Considere uma aplicação de streaming de vídeo armazenado, como por exemplo, o YouTube. Responda às perguntas abaixo.

1. (0.5 ponto) Explique por que o vídeo "congela" subitamente durante sua reprodução no cliente.

   Resposta: O vídeo "congela" subitamente porque pacotes de dados deixam de chegar ao cliente. Com isto, o buffer do lado do cliente se esvazia e o cliente não há mais o que reproduzir, sendo o congelmaneto a única opção.

2. (0.5 ponto) Considere o retardo entre o instante em que o vídeo congela e o instante em que o vídeo reinicia sua reprodução no cliente. Quais são os motivos deste retardo?

   Resposta: Este retardo é causado pela rede e pelo tempo de bufferização. No instante que o vídeo congela, pacotes que ainda não chegaram ao cliente estão a caminho, na rede. Ao chegarem, eles são colocados em um buffer do lado do cliente, até que um número suficientemente grande chegue. Somente após esta re-bufferização, que pode demorar um tempo, o cliente inicia a reprodução novamente.

3. (0.5 ponto) Considere a técnica de bufferização do lado do cliente. Cite uma vantagem e uma desvantagem de se utilizar um tamanho de buffer muito pequeno?

   Resposta: Ao utilizar um buffer muito pequeno o risco do buffer esvaziar e o vídeo congelar é maior, pois o cliente ficará mais sensível aos atrasos da rede. Ou seja, um atraso relativamente pequeno nos pacotes em transmissão pode zerar o buffer que é pequeno, sendo assim uma desvantagem. Por outro lado, o buffer pequeno demanda menos tempo para ser preenchido, podendo a reprodução iniciar mais rapidamente, após a chegada de poucos pacotes. Esta vantagem está presente tanto no início da reprodução, quanto depois de um congelamento.

5ª questão (2.0 pontos)

Segurança em redes. Considere as seguintes informações criptográficas:

- Sejam K_A^+ e K_A^- as chaves públicas e privadas de Ana, respectivamente.
- Sejam K_B^+ e K_B^- as chaves públicas e privadas de Bruno, respectivamente.
- Seja $H(\cdot)$ uma função de *hash* utilizada para gerar *message digests* (resumos de mensagens).
- Seja m uma mensagem em texto que Ana deseja enviar a Bruno.
- Assuma que Ana e Bruno (e qualquer outra pessoa) possuam todas as chaves públicas.

Responda às perguntas abaixo:

1. (1.0 ponto) Considere que Ana enviou a Bruno as seguintes três mensagens criptográficas: $M_1 = K_B^+(H(m))$, $M_2 = H(K_A^+(m)))$, $M_3 = K_A^+$. Bruno irá conseguir ler a mensagem m que Ana deseja lhe enviar? Analise e explique cada uma das mensagens criptográficas enviadas por Ana.

   Resposta: Não, Bruno não irá conseguir ler a mensagem m. A primeira mensagem enviada, M_1 possui apenas o hash da mensagem m e Bruno não consegue recuperar m

a partir de $H(M)$. A segunda mensagem enviada também é o um hash, e Bruno não irá conseguir recuperar a mensagem m. A terceira mensagem é apenas a chave pública de Ana, a qual Bruno já possui, pois assumimos que todos possuem as chaves públicas. Logo neste caso, Bruno não consegue ler m.

2. (1.0 ponto) Considere que Ana enviou a Bruno as seguintes três mensagens criptográficas: $M_1 = K_B^+(K_A^-)$, $M_2 = K_A^+(m)$, $M_3 = H(m)$. Bruno irá conseguir ler a mensagem m que Ana deseja lhe enviar? Analise e explique cada uma das mensagens criptográficas enviadas por Ana.

   Resposta: Sim. Bruno irá conseguir ler m. Na primeira mensagem, Bruno recebe a chave privada de Ana cifrada com sua chave pública. Ao aplicar sua chave privada, Bruno irá conseguir obter a chave privada de Ana, pois $K_B^-(M_1) = K_B^-(K_B^+(K_A^-)) = K_A^-$. Na segunda mensagem, Ana cifrou m utilizando sua chave pública. Desta forma, Bruno pode decifrar esta mensagem utilizando a chave privada de Ana, obtida com M_1. Ou seja, $K_A^-(M_2) = K_A^-(K_A^+(m)) = m$, e desta forma Bruno obtem m. Por fim, repare que a terceira mensagem eviada por Ana não é necessária para decifrar m, mas pode ser utilizada para verificar a integridade de m obtida com M_2, pois M_3 possui o hash de m, que pode ser comparado com o hash da m decifrada. Apesar de Bruno conseguir ler a mensagem m, o procedimento acima utilizado por Ana não é adequado, pois Ana revelou a Bruno sua chave privada. Desta forma, Bruno poderá ler qualquer outra mensagem que seja cifrada com a chave pública dela.