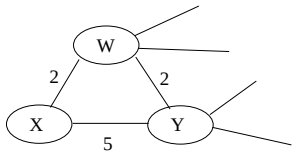
Fundação CECIERJ - Vice Presidência de Educação Superior a Distância

Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP3 - 1° semestre de 2011

1ª questão (2.5 pontos)

Algoritmos de Roteamento. Considere uma parte de uma rede conforme apresentada na figura abaixo. **X** tem dois vizinhos, **W** e **Y**. O custo mínimo de **W** até o destino **U** é de 5 e o custo mínimo de **Y** até **U** é de 6. O caminho completo de **Y** e **W** até **U** não é mostrado na figura.



Responda as perguntas abaixo explicando como você as obteve.

1. (0.6) Construa o vetor de distâncias de **X** para os destinos **W**, **Y** e **U**.

   Resposta:

   O vetor de distâncias inicial do nó X só contém as distâncias de X até os vizinhos. Abaixo encontram-se os vetores de distância dos nós da rede:

   Nó X

W	2
Y	5
U	∞

   Nó W

X	2
Y	2
U	5

   Nó Y

X	4
W	2
U	6

   Após uma troca de mensagens, o vetor de distâncias de X é:

   Nó X

W	2
Y	4
U	7

   Este é o vetor final de X, pois após a próxima troca de mensagens, o vetor de distâncias de X não se modificará.

2. (0.6) Suponha que houve uma alteração no custo do enlace (**X**, **W**) e que agora o novo valor do custo é de 4. Neste caso qual seria o novo vetor de distâncias de **X** ? Que mensagem **X** enviaria para seus vizinhos ?

   Resposta:

   O vetor de distâncias de X será:

   Nó X

W	4
Y	4
U	7

   X enviará para os seus vizinhos uma mensagem com o seu novo vetor de distâncias.

3. (1.3) Considere agora que houve uma alteração no custo do enlace (**X**, **W**) e que o novo valor do custo é de 50. Neste caso quais seriam os novos vetores de distâncias de **X**, **W** e **Y** após uma única troca de mensagem entre os nós ? Neste cenário ocorreria o problema contagem ao infinito ? Justifique.

   Resposta:

Estes são os vetores de distâncias antes da mudança do custo do enlace (W,X):

Nó X

W	2
Y	4
U	7

Nó W

X	2
Y	2
U	5

Nó Y

X	4
W	2
U	6

Após o custo do enlace (W,X) mudar de 2 para 50, o vator de distâncias de X será:

Nó X

W	7
Y	5
U	11

X envia seu novo vetor de distâncias para os vizinhos (primeira troca de mensagens). O novo vetor de distâncias dos vizinhos será recalculado e será o seguinte:

Nó W

X	6
Y	2
U	5

Nó Y

X	4
W	2
U	6

Neste cenário não ocorre o problema contagem até o infinito. Após a próxima troca de mensagens os vetores de distância vão convergir para o valor correto.

$2^{\underline{a}}$ questão (2.5 pontos)

Camada de rede. Responda as questões abaixo:

1. (1.0) Suponha que você tenha um roteador/modem na sua casa para acesso a Internet e que seu provedor atribui um único endereço IP ao seu roteador/modem. Considere que você quer conectar 4 computadores simultaneamente a Internet. Explique sucintamente que técnica pode ser usada para permitir a conexão de múltiplos computadores através do roteador/modem que possui um único endereço IP.

   Resposta:

   A técnica que pode ser usada é chamada NAT. O NAT é um mecanismo que permite criar uma rede local privada, com endereços IPs que não são vistos diretamente por hosts na Internet pública. O roteador com NAT permite que um computador na rede local privada faça uma conexão com um host na rede pública da Internet, traduzindo os endereços. Quando um computador abre uma conexão TCP com um servidor Web na Internet, por exemplo, o roteador com NAT anota o endereço e a porta de origem do pacote vindo da rede local privada, e muda a porta e o endereço do pacote antes de transmiti-lo pelo link de saída (que dá acesso a Internet). O roteador com NAT mantém uma tabela com este mapeamento. O novo endereço de origem deste pacote é o endereço IP público do roteador com NAT.

2. (1.5) Considere uma rede que opera por datagrama e usa 8 bits para endereçar os computadores. Suponha que o roteador faça o encaminhamento usando o prefixo mais longo (*longest prefix matching*) e que possua a tabela abaixo:

Prefixo	Interface
1	0
10	1
111	2
outros	3

Forneça o intervalo de endereços destino de hosts (*destination host adresses*) associado a cada uma das interfaces e o número de endereços contidos no intervalo.

Resposta:

Nas respostas abaixo foram tirados 2 endereços de hosts que correspondem aos endereços onde os bits do ultimo octeto (usado para endereçar os hosts) são todos iguais a zero ou todos iguais a um.

Interface 0:

Endereços destino: 192.0.0.1 a 223.255.255.254

Números de endereços: $(32 \times 2^8 \times 2^8)$ endereços de rede e cada rede pode endereçar (2^8-2) máquinas.

Interface 1:

Endereços destino: 128.0.0.1 a 191.255.255.254

Números de endereços: $(64 \times 2^8 \times 2^8)$ endereços de rede e cada rede pode endereçar (2^8-2) máquinas.

Interface 2:

Endereços destino: 224.0.0.1 a 255.255.255.254

Números de endereços: $(32 \times 2^8 \times 2^8)$ endereços de rede e cada rede pode endereçar (2^8-2) máquinas.

Interface 3:

Endereços destino: 0.0.1.1 a 126.0.0.1

Números de endereços: $((127 \times 2^8 \times 2^8) - 1)$ endereços de rede e cada rede pode endereçar (2^8-2) máquinas. Foi tirado 1 endereço de rede correspondente a todos os bits dos três primeiros octetos iguais a zero.

$3^{\underline{a}}$ questão (2.0 pontos)

Camada de Enlace: O MTU (*Maximum Transmission Unit*) é uma importante característica dos enlaces de rede. Responda às perguntas abaixo.

1. (0.5 pontos) Determine quando e por que é necessário fragmentar um datagrama para que o mesmo seja transmitido por um determinado enlace.

   Resposta: Todo enlace de rede possui um MTU que é a maior quantidade de bytes de dados (*payload*) que podem ser transmitidos por um quadro naquele enlace. Este valor pode ser menor do que a quantidade de bytes de um datagrama proveniente da camada de redes. Neste caso, o datagrasma precisa ser fragmentado e transmitido em múltiplos quadros diferentes. Em particular, o datagrama será framentado em pedaços de MTU bytes cada.

2. (0.5 pontos) Por que o MTU de um enlace não deve ser muito pequeno?

   Resposta: Porque senão teremos um *overhead* muito grande. Dentro da área de dados (*payload* do quadro, cujo tamanho máximo é dado pelo MTU, teremos o cabeçalho das camadas de rede e transporte (ex. IP e TCP), sobrando ainda menos espaço para os dados do usuário. Se o MTU for muito pequeno, teremos um overhead muito grande, uma vez que o overhead é dado por C/MTU, onde C é o tamanho em bytes do cabeçalho das camadas de redes e transporte. Neste caso, estaremos utilizando grande parte da capacidade de transmissão do canal para transmitir cabeçalhos e não dados do usuário.

3. (0.5 pontos) O padrão Ethernet utiliza um MTU de 1500 bytes. Considere a transmissão de um arquivo de 3.5MB (1MB = 10^6 bytes) por um enlace Ethernet. Considerando o cabeçalho dos protocolos IP e TCP (que contém 20 bytes cada), determine quantos quadros Ethernet são necessários para transmissão do arquivo.

   Resposta: Como o cabeçalho do datagrama que irá chegar a camada de enlace possui $20 + 20 = 40$ bytes, teremos efetivamente espaço para $1500 - 40 = 1460$ bytes de dados em cada quadro, uma vez que o MTU do Ethernet é de 1500 bytes. Assim sendo, iremos precisar de $\lceil 3.5 * 10^6/1460 \rceil = 2398$ quadros para transmitir o arquivo, sendo que o último quadro terá apenas $3.5 * 10^6 - (2397 * 1460) = 380$ bytes do arquivo.

4. (0.5 pontos) O *overhead* depende do tamanho do arquivo sendo transmitido? Lembrando que o *overhead* é a razão entre o total de bytes de cabeçalho e total de bytes transmitidos.

   Resposta: Não, o overhead não depende do tamanho do arquivo, pois todo quadro possui dentro do seu payload o cabeçalho das camadas de rede e de transporte. No caso acima, o overhead é dado por $C/MTU = 40/1500 = 2.6\%$ e independe do tamanho do arquivo.

$4^{\underline{a}}$ questão (1.0 pontos)

Aplicações Multimída: Considere uma aplicação de streaming de vídeo em tempo real. Responda às perguntas abaixo.

1. (0.5 ponto) Explique por que a técnica de bufferização do lado do cliente melhora a qualidade do vídeo exibido no cliente.

   Resposta: Porque reduz o *jitter* experimentado pela aplicação. Ou seja, ao armazenar os pacotes em um buffer antes de começar a serem decodificados, temos uma chance menor de precisarmos decodificar um pacote que ainda não chegou devido a atrasos na rede. Com isto temos menos falhas no fluxo de vídeo, melhorando sua qualidade.

2. (0.5 ponto) Explique por que o uso de redundância melhora a qualidade do vídeo exibido no cliente?

   Resposta: Porque reduz a perda de pacotes experimentada pela aplicação. Ou seja, ao usarmos redundância, um pacote descartado pela rede pode ser recuperado do lado do cliente utilizando a redundância que chegou juntamente com outros pacotes. Com isto teremos menos falhas no fluxo de vídeo, melhorando sua qualidade.

$5^{\underline{a}}$ questão (2.0 pontos)

Segurança em Redes: Responda às perguntas abaixo.

1. (1.0 ponto) Segurança em redes é obtida garantindo algumas propriedades na comunicação entre duas entidades. Explique sucintamente o que significa cada uma das propriedades abaixo.

   - Autenticidade

     Resposta: Ter conhecimento da real identidade da entidade com a qual estamos comunicando. Ou seja, a autenticidade na comunicação entre A e B nos garante que A está se comunicando com B e não com uma outra entidade C que se faz passar por B.

   - Integridade

     Resposta: Garantir que o os dados rececibos foram realmente os transmitidos. Ou seja, a integridade na comunicação entre A e B nos garante que se B recebe M de A, então A realmente transmitiu M para B, ou seja, esta mensagem não foi alterada em sua transmissão.

   - Confidencialidade

     Resposta: Garantir que apenas as entidades que se comunicam tem conhecimento do real conteúdo da informação sendo transmitida. Ou seja, confidencialidade na comunicação entre A e B nos garante que apenas A e B tem conhecimento do real conteúdo de uma mensagem M transmitida entre eles.

2. (1.0 ponto) Mostre como podemos obter confidencialidade. Assuma que Ana deseja enviar uma mensagem confidencial para Bruno. Descreva todos os passos necessários neste processo.

   Resposta: Temos duas formas de obter confidencialidade na comunicação entre Ana e Bruno: utilizando chaves simétricas ou chaves público/privadas. Confidencialidade baseada em chave simétrica assume que Ana e Bruno compartilham um segredo, por exemplo K_S. Este segredo é a chave de um algoritmo de criptografia simétrico. Para transmitir M, Ana deve cifrar a mensagem usando K_S e transmitir $K_S(M)$ para Bruno. Ao receber a mensagem cifrada, Bruno decifra a mensagem usando a mesma chave K_S, obtendo M de volta. Confidencialidade baseada em chave pública/privada assume que Ana possui a chave pública de Bruno, K_B^+, e Bruno possui a chave pública de Ana, K_A^+. Para transmitir M, Ana deve cifrar a mensagem usando a chave pública de Bruno e transmitir $K_B^+(M)$ para Bruno. Ao receber a mensagem cifrada, Bruno decifra a mensagem usando sua chave privada, obtendo M de volta.