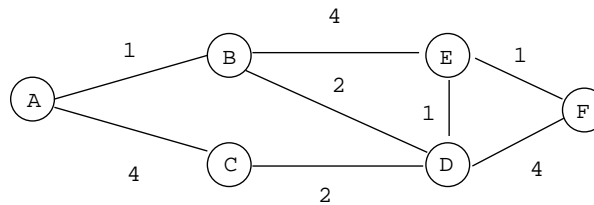


Fundação CECIERJ - Vice Presidência de Educação Superior a Distância  
**Curso de Tecnologia em Sistemas de Computação**  
**Disciplina: Redes de Computadores II**  
**Gabarito da AP3 - 2º semestre de 2010**

**1ª questão (3.0 pontos)**

**Algoritmos de Roteamento**

Considere a rede de comunicação da figura abaixo. O algoritmo de roteamento usado na rede é o *Distance Vector Routing* (vetor de distâncias que é baseado no Bellman-Ford).



- (1.0 ponto) Explique como funciona este protocolo, isto é, indique os passos principais para atualização das tabelas.

**Resposta:**

A tabela de roteamento de um nó X pode ser atualizada quando: (i) X recebe um novo vetor de distâncias de um dos seus vizinhos ou (ii) quando o custo de um de seus enlaces de saída se altera. Caso (i) ou (ii) ocorra, X recalcula o seu vetor de distâncias (conforme equação abaixo). Se existir alguma alteração, envia o novo vetor para seus vizinhos.

- (1.5 pontos) Em um determinado instante as tabelas de roteamento dos nós da rede são as seguintes:

NÓ B		NÓ C		NÓ E		NÓ F	
A	2	A	3	A	6	A	7
B	0	B	5	B	3	B	4
C	4	C	0	C	4	C	4
D	2	D	2	D	2	D	3
E	3	E	4	E	0	E	2
F	3	F	5	F	2	F	0

Construa a tabela de roteamento do nó D considerando as tabelas e a topologia da rede das figuras acima. EXPLIQUE.

**Resposta:**

Cada nó  $x$  da rede constrói a tabela de roteamento a partir da seguinte equação:

$$D_x(y) = \min_v \{c(x, v) + D_v(y)\} \text{ para cada nó } y \text{ pertencente a rede.}$$

onde  $c(x, v)$  é o custo do enlace que liga  $x$  a um vizinho seu  $v$ ,  $D_x(y)$  é a distância de  $x$  até um nó  $y$  da rede e  $D_v(y)$  é a distância de  $v$  até um nó  $y$  da rede.

$x$  usa o último vetor de distâncias  $D_v$  recebido de seus vizinhos  $v$  e o último valor que estimou para  $c(x, v)$ , para calcular o seu vetor de distâncias  $D_x$ .

Usando a equação acima e as tabelas dos vizinhos de D (tabelas dos nós B,C,e,F) temos a tabela de D conforme abaixo:

Tabela do nó D

A	4
B	2
C	2
E	1
F	3

3. (0.5 ponto) Cite um problema que pode ocorrer com este algoritmo se um enlace da rede tem um aumento significativo no seu custo.

**Resposta:**

Pode ocorrer o problema *contagem até o infinito*, ou seja, as tabelas dos nós demorarão para convergir até que o melhor caminho até um certo destino seja encontrado. Até que o caminho seja encontrado, os pacotes poderão ficar em *loop* e não chegarão ao seu destino.

## 2ª questão (1.0 ponto)

### Protocolo ARP

Considere na rede da figura abaixo que o *host* A quer enviar uma mensagem para o *host* B. Suponha que a tabela ARP de A esteja vazia. Descreva as mensagens trocadas na rede (pelo protocolo ARP) até que A possua as informações necessárias para enviar a mensagem para B.

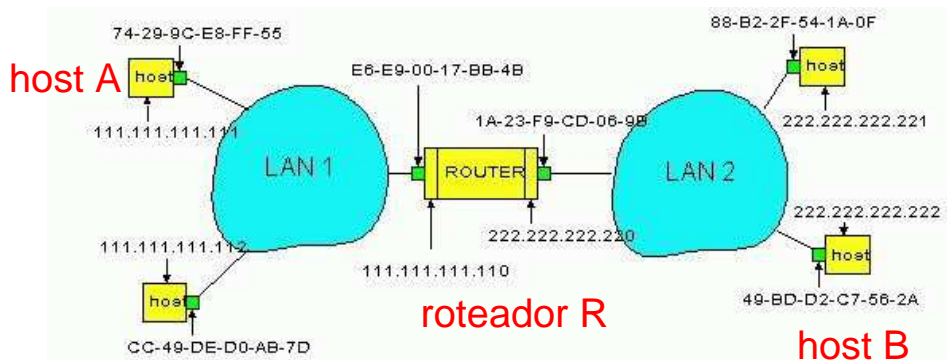
**Resposta:**

Passo 1: A envia pacote ARP query em broadcast contendo endereço IP do roteador pois descobre através da sua tabela de roteamento IP que B 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.

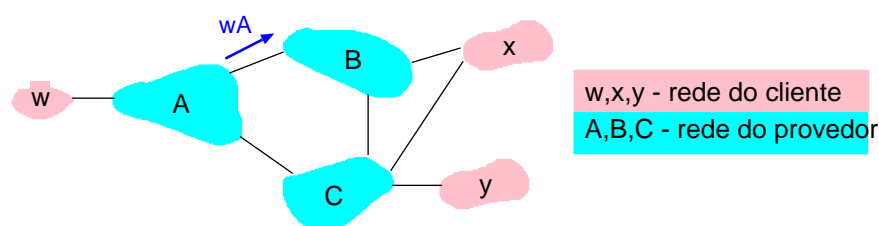
Passo 3: A recebe o pacote do roteador e atualiza a sua tabela ARP criando uma entrada com o endereço IP do roteador e o respectivo MAC. A envia quadro cujo endereço MAC de destino é o MAC do roteador. Neste quadro, A encapsula o pacote destinado a B (IP destino é B).

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



### 3ª questão (1.0 ponto)

#### BGP



Considere na rede da figura acima que o provedor A está anunciando a rota  $wA$  para o provedor B. Responda as perguntas abaixo como se você fosse o administrador do provedor B. Ou seja, que tipo de política de anúncio de rotas você implementaria para esta rota divulgada por A. Note que os clientes de A são da rede  $w$ , os clientes de B são da rede  $x$  e os clientes de C são das redes  $x$  e  $y$ .

1. (0.5 pontos) Você anunciaria a rota  $wA$  para  $x$  ? Por quê ?

#### Resposta:

Sim, pois os clientes da rede  $x$  são clientes do provedor B e estão pagando a B para ter acesso a Internet.

2. (0.5 pontos) Você anunciaria a rota  $wAB$  para  $C$  ? Por quê ?

#### Resposta:

Não, pois  $C$  é outro provedor e não interessa para B rotear tráfego dos clientes de  $C$  porque B não receberá nada por rotear este tráfego.

### 4ª questão (1.0 ponto)

#### Endereçamento IP.

Considere um roteador que interconecta três sub-redes: sub-rede A, sub-rede B, e sub-rede C. Suponha que todas as interfaces destas sub-redes precisam estar dentro da seguinte faixa de endereço  $118.210.20.128/25$ . Suponha também que a sub-rede A tenha que suportar 30 interfaces, a sub-redes B 25 interfaces, e a subrede 20 interfaces. Forneça três faixas de endereços da forma  $a.b.c.d/x$ , uma faixa para cada sub-rede, de forma a atender as restrições acima. Explique sua resposta.

#### Resposta:

Para diferenciar entre as três redes, podemos utilizar os dois próximos bits disponíveis dentro da faixa de endereços 118.210.20.128/25. Ou seja, usamos os bits 26 e 27 para identificar cada uma das 3 redes locais. A rede  $L_1$  pode ficar com "0\*" para estes dois bits, ou seja, bit 26 = 0, dando origem a uma rede /26, ou seja, 118.210.20.128/26. Repare que neste caso, o bit 27 pertence ao endereçamento dos hosts. Desta forma, a rede  $L_1$  terá 6 bits para endereçamento dos hosts, totalizando  $2^6 = 64$  endereços diferentes. A subrede  $L_2$  pode ficar com "10" e a rede  $L_3$  com "11" para os bits 27 e 28, respectivamente. Repare que isto dá origem a uma rede /27, ou seja, 118.210.20.192/27 e 118.210.20.224/27, respectivamente. Desta forma, sobram 5 bits para endereçamento dos hosts destas redes, totalizando  $2^5 = 32$  endereços diferentes em cada subrede, atendendo assim as exigências do problema.

## 5ª questão (2.0 pontos)

**Camada de Enlace:** Responda às perguntas abaixo.

1. (0.5 ponto) Qual é a principal vantagem e desvantagem dos protocolos baseados na partição do canal, como TDMA e FDMA?

**Resposta:**

A principal vantagem é que estes protocolos estão livres de colisão e por isto garantem o acesso ao canal em tempo determinístico, assim como garantem a banda que cada usuário irá receber. A principal desvantagem é a baixa utilização do canal quando temos poucos usuários compartilhando o mesmo, uma vez que os recursos são dedicados e não podem ser utilizados por outros usuários. Outra desvantagem é a complexidade de operar e gerenciar o protocolo perante uma constante variação no número de usuários que compartilham o canal.

2. (0.5 ponto) Qual é a principal vantagem e desvantagem dos protocolos baseados no acesso aleatório, como ALOHA e CSMA?

**Resposta:**

A principal vantagem é a baixa complexidade de implementação e a facilidade com que eles se adaptam a uma variação no número de usuários que utilizam o canal. Em particular, o canal é compartilhado pelos usuários que necessitam, dando origem a um bom desempenho quando a rede possui poucos usuários. A desvantagem são as colisões que afetam o desempenho do protocolo quando o número de usuários é muito elevado.

3. (1.0 ponto) Explique porque o protocolo Slotted-ALOHA é mais eficiente que o protocolo ALOHA. Dica: use uma figura para ilustrar sua resposta.

**Resposta:**

O protocolo Slotted-ALOHA trabalha com slots do tempo e as estações estão sincronizadas e só podem transmitir no início de um slot. Desta forma, em caso de colisão, exatamente um slot de tempo será perdido, pois o tempo de transmissão dura exatamente o tempo de um slot. No protocolo ALOHA as estações podem transmitir a qualquer instante sem antes verificar se há uma transmissão em curso. Desta forma, uma estação pode iniciar sua transmissão um pouco antes de outra terminar sua transmissão. Logo, teremos uma colisão e as duas transmissões serão perdidas. Repare que neste caso o tempo desperdiçado foi o tempo de duas transmissões, o que sempre acontece quando uma colisão ocorre. Logo, o protocolo Slotted-ALOHA é mais eficiente, pois desperdiça menos tempo quando ocorre uma colisão.

## 6ª 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:**

Autenticidade é a propriedade que garante que a comunicação está ocorrendo entre as partes que realmente desejam se comunicar. Ou seja, garante que uma determinada entidade conhece e tem certeza da identidade da outra entidade com a qual ela está se comunicando.

- Integridade

**Resposta:**

Integridade garante que a informação não é alterada durante sua transmissão. Ou seja, garante que será possível detectar qualquer tipo de alteração na informação durante sua transmissão.

- Confidencialidade

**Resposta:**

Confidencialidade garante que a informação original não pode ser obtida por uma terceira entidade. Ou seja, somente a entidade desejada (destinatário) terá acesso à informação original e caso a informação transmitida seja interceptada esta não poderá ser transformada na informação original.

2. (1.0 ponto) Explique como o uso de um *nonce* evita o *ataque de playback* durante o processo de autenticação.

**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 autenticar *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 a 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*).