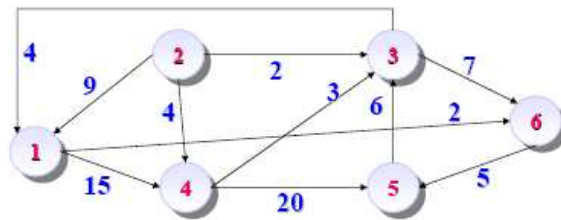


Fundação CECIERJ - Vice Presidência de Educação Superior a Distância
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP3 - 2º semestre de 2009

1ª questão (3.0 pontos)

Considere a rede de comunicação da figura abaixo:



1. (0.8) Explique sucintamente como funciona o algoritmo de roteamento *Link State*. Na sua resposta, não esqueça de indicar: quando são trocadas informações entre os roteadores e que tipo de informação é trocada; como um roteador computa as informações necessárias para obter a tabela de roteamento.

Resposta:

Cada nó armazena a topologia da rede e executa o algoritmo de Dijkstra para cálculo do menor caminho até todos os destinos da rede.

O nó executa o algoritmo de Dijkstra quando um dos seguintes eventos ocorre: (i) mudança no custo de um dos seus enlaces de saída ou (ii) recebimento de mensagem de um outro nó da rede indicando alteração na topologia (ex: custo de um enlace).

Após a execução do algoritmo, caso o custo ou o enlace de saída para algum destino na rede mude, o nó atualiza a sua tabela de roteamento.

O nó envia mensagem para todos os outros nós usando o algoritmo de flooding caso o custo de algum de seus enlaces de saída se altere. A mensagem contém a identificação do nó e o custo de cada um dos seus enlaces de saída.

2. (1.0) Construa a tabela de roteamento do nó 1 da rede indicando os passos usados na sua construção.

Resposta:

O resultado do processo iterativo (algoritmo de Dijkstra) está ilustrado na tabela abaixo:

Passo	N'	d(2),p(2)	d(3),p(3)	d(4),p(4)	d(5),p(5)	d(6),p(6)
0	1	9,1	4,1	15,1	∞	2,6
1	1,6	9,1	4,1	15,1	7,6	-
2	1,6,3	6,3	-	7,3	7,6	-
3	1,6,3,2	-	-	7,3	7,6	-
4	1,6,3,2,4	-	-	-	7,6	-
5	1,6,3,2,4,5	-	-	-	-	-

A tabela de roteamento do nó 1 é facilmente contruída a partir da tabela acima.

Tabela de roteamento do nó A:

Destino	Enlace de Saída
2	1,3
3	1,3
4	1,3
5	1,6
6	1,6

3. (0.6) Faça uma comparação entre os algoritmos *Link State Routing* e *Distance Vector Routing* em termos de: (i) destino e conteúdo das mensagens trocadas entre os nós, (ii) informações armazenadas pelos nós, (iii) problemas que podem ocorrer com os algoritmos.

Resposta:

- (a) destino e conteúdo das mensagens trocadas entre os nós

Link State Routing: Mensagens são enviadas de um nó i para todos os nós da rede e contém o custo dos enlaces do nó i .

Distance Vector Routing: Mensagens são enviadas de i para seus vizinhos e contém a tabela de roteamento de i , ou seja, o custo de i para todos os destinos da rede.

- (b) informações armazenadas pelos nós

Link State Routing: cada nó i armazena a topologia da rede.

Distance Vector Routing: cada nó i armazena os custos até os seus vizinhos.

- (c) problemas que podem ocorrer com os algoritmos

Link State Routing: problema de oscilação de roteamento, ora o rota de todos os nós e feita no sentido horário, ora e feita no sentido anti-horário.

Distance Vector Routing: problema de contagem até o infinito.

4. (0.6) Descreva o que é o problema contagem até o infinito (*count to infinity problem*) e em que cenário ele pode ocorrer.

Resposta:

O problema *contagem até o infinito* é caracterizado pela demora na convergência das tabelas de roteamento dos nós. Enquanto as tabelas não estiverem corretas, os nós utilizam rotas incorretas que podem levar os pacotes a ficarem em *loop*. Ele ocorre quando o custo de um determinado enlace aumenta significativamente de valor.

2ª questão (2.5 pontos)

1. (0.8) 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 estações 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.

2. (0.6) 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.

3. (0.5) Indique uma vantagem do uso das mensagens de reserva **CTS** e **RTS** pelo protocolo de acesso sem fio IEEE802.11.

Resposta:

Uma vantagem é que quando as mensagens de reserva são menores que as mensagens de dados, o tempo de colisão é menor, o que aumenta o tempo que o canal transmite informação útil (melhora o desempenho do protocolo).

4. (0.6) Suponha uma rede sem fio IEEE802.11 onde duas estações A e B transmitem e suas mensagens colidem. Como as estações detectam que suas mensagens colidiram e não chegaram corretamente no destino ?

Resposta:

A estação detecta que houve colisão ou que suas mensagens não chegaram corretamente no destino quando não recebe uma mensagem de ACK do receptor.

3ª questão (1.0 pontos)

Suponha que um roteador da Internet com possua a seguinte tabela de roteamento:

Indique para qual porta de saída os pacotes com os seguintes endereços destino serão encaminhados:

128.119.121.100

128.119.121.150

Prefixo	Interface
128.119.121.0/24	0
128.119.121.192/26	1
caso contrário	2

128.119.121.200

Resposta:

128.119.121.100 – Porta 0

128.119.121.150 – Porta 0

128.119.121.200 – Porta 1

4ª questão (2.0 pontos)

Acesso ao Meio: Responda às perguntas abaixo.

1. (1.0) Compare os protocolos de acesso aleatório ALOHA e Slotted-ALOHA indicando apenas suas diferenças. Explique porque um deles é em geral mais eficiente do que o outro.

Resposta:

A principal diferença entre os dois protocolos está no fato de que no Slotted ALOHA as estações que compartilham o meio estão todas sincronizadas e só iniciam uma transmissão exatamente no início de um slot de tempo. Uma colisão dura exatamente um slot de tempo. No protocolo ALOHA as estações não estão sincronizadas, podendo assim iniciar sua transmissão em qualquer instante de tempo. O protocolo Slotted ALOHA é em geral mais eficiente, ainda mais quando assumimos um cenário de alta carga (ou seja, muitas estações querendo transmitir). Este protocolo é mais eficiente pois em caso de colisão o canal é desperdiçado apenas por um slot de tempo, enquanto que no ALOHA convencional, uma colisão pode desperdiçar o tempo equivalente a dois slots (duas transmissões).

2. (1.0) Compare os protocolos de acesso aleatório CSMA e CSMA-CD indicando apenas suas diferenças. Explique porque um deles é em geral mais eficiente do que o outro.

Resposta:

A principal diferença entre os dois protocolos está no fato de que o protocolo CSMA-CD (*collision detection*) detecta a colisão assim que ela ocorre abortando a transmissão do quadro logo em seguida. Este procedimento não é adotado no protocolo CSMA, que transmite o quadro até o final para somente depois verificar se houve uma colisão. O protocolo CSMA-CD é em geral mais eficiente, ainda mais quando assumimos um cenário de alta carga (ou seja, muitas estações querendo transmitir). Este protocolo é mais eficiente pois em caso de colisão o canal é desperdiçado apenas até que a colisão seja detectada, enquanto que no CSMA convencional, uma colisão pode desperdiçar o tempo equivalente a uma transmissão de quadro.

5ª questão (1.5 pontos)

Multimídia e Segurança: Responda às perguntas abaixo.

1. (0.5) Considere uma aplicação de transmissão de vídeo armazenado por *streaming*. Cite uma vantagem e uma desvantagem da técnica de bufferização do lado do cliente.

Resposta:

Vantagens: reduz o jitter para a aplicação (ou seja, reduz a variação do atraso entre os pacotes); permite a aplicação oferecer melhor qualidade ao usuário. Desvantagens: aumenta o retardo entre o instante que o usuário solicita o conteúdo (vídeo) e o instante em que o usuário efetivamente começa a visualizar e/ou ouvir o conteúdo. Este atraso é conhecido como *playout delay*.

2. (0.5) De forma geral, o *message digest* de uma mensagem M nada mais é do que um “resumo” de M . Como podemos obter este resumo? Para que serve este resumo?

Resposta:

O *message digest* é geralmente gerado utilizando alguma função de *hash* (função de espalhamento), como MD5 ou SHA, que geram resumos de tamanho fixo (ex. 128 bits). Este resumo é utilizado como primitiva criptográfica para garantir a integridade de uma mensagem. Ou seja, para garantir que os bits da mensagem não foram alterados por acaso ou maliciosamente durante a transmissão. Uma mensagem M é transmitida juntamente com seu resumo $h(M)$. O receptor então verifica se o resumo da mensagem recebida, ou seja $h(M')$, onde M' é a mensagem recebida, é igual ao resumo recebido, ou seja $h(M)$. Caso negativo, a mensagem foi alterada durante sua transmissão.

3. (0.5) Explique porque o uso de um *nonce* evita o ataque de playback durante o processo de autenticação.

Resposta:

Considere o cenário onde a entidade A deseja autenticar a entidade B (ou seja, A deseja ter certeza de que está se comunicando com B). O *nonce* é um número gerado pela entidade A toda vez que uma autenticação precisa ser feita. Este número é gerado aleatoriamente (ou pseudo-aleatoriamente) e utilizado apenas uma vez por A . Em particular, A transmite este número a B que deve então cifrá-lo utilizando uma chave simétrica e transmitir o resultado de volta para A . A entidade A então verifica que B realmente cifrou o número que acabou de ser gerado, evitando assim um ataque de playback.