Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP3 – 1º semestre de 2015 – GABARITO

Questão 1 ..... 10 pontos

Na tabela abaixo, são apresentados, nas colunas, diversos protocolos de acesso a um meio de transmissão compartilhado, e nas linhas, diversas características destes protocolos. Preencha cada célula da tabela indicando se o protocolo possui ou não a característica apresentada. Considere que, exceto em afirmação contrária, a quantidade de estações que possuem acesso ao meio em questão é constante (isto é, estações não entram e saem da rede), mas que nem todas as estações desejam transmitir a todo instante.

	S-ALOHA	CSMA	CDMA	ALOHA
o meio somente pode atingir utilização de 100% se todas as estações quiserem transmitir	×	×	✓	×
o meio pode ficar ocioso mesmo se estações quiserem iniciar novas transmissões	✓	×	×	×
protocolo de acesso aleatório	✓	✓	×	✓
permite acesso simultâneo ao meio (causando colisão)	✓	✓	×	✓
a adição de uma estação adicional que não transmite reduz a utilização do meio	×	×	×	×

Questão 2 ..... 20 pontos

Considere as afirmações abaixo sobre transmissões multimídia. Para cada afirmação, indique se a mesma é verdadeira ou falsa, e explique sua resposta utilizando *apenas uma frase*:

√ **Um pacote de uma aplicação *streaming* que chega no receptor depois do tempo que foi escalonado para tocar é considerado um pacote perdido.**
Um pacote que chega atrasado não pode ser tocado pois, para que a qualidade de uma aplicação multimídia seja mantida, os pacotes devem ser tocados seguindo o mesmo intervalo de tempo em que foram gerados.

◯ O protocolo TCP provê um serviço que garante confiabilidade e entrega em ordem de todos os pacotes para a aplicação. Essas garantias permitem oferecer uma boa qualidade para aplicações de voz.
O principal requisito para que uma aplicação de voz tenha boa qualidade é que o retardo e jitter estejam sempre abaixo de um determinado valor.

◯ A técnica de interleaving insere redundância no fluxo de pacotes transmitidos e

portanto aumenta a taxa de transmissão da aplicação.
A técnica de interleaving consiste na divisão dos pacotes originais em pedaços e reorganização desses pedaços construindo os novos pacotes que serão transmitidos, de forma que não é inserida nenhuma informação redundante.

◯ No mecanismo de bufferização do lado do cliente, quanto menor for o *buffer* do usuário, menor será o números de pausas que ocorrerão devido ao esvaziamento do *buffer*.
Quanto menor for o *buffer*, maior será o número de pausas, pois maior será a chance do *buffer* esvaziar e ocorrer a pausa.

√ **A técnica de interleaving tem como desvantagem o aumento da latência.**
Na técnica de interleaving cada pacote transmitido é composto de n pedaços, sendo que cada pedaço é uma parte de um pacote do fluxo original. Logo, para o receptor tocar um pacote do fluxo original, ele deve aguardar a chegada de n pacotes.

Questão 3 ..... 10 pontos

Na coluna à direita, são apresentadas características de protocolos de roteamento. Associe cada característica a um dos protocolos da coluna da esquerda.

(LS) Estado de enlace
(DV) Vetor de distâncias

(**LS**) Cálculo de rotas baseado em algoritmos como Prim ou Dijkstra
(**LS**) Roteadores calculam as rotas de maneira independente
(**DV**) Informações topológicas da rede são trocadas apenas entre vizinhos imediatos
(**DV**) Atinge melhor desempenho com a ajuda de técnicas como envenenamento reverso
(**LS**) Implementado nos protocolos OSPF e IS-IS
(**LS**) Mapa topológico da rede é utilizado pelo cálculo de rotas
(**DV**) Cálculo distribuído de rotas
(**DV**) Tabela de distâncias é utilizada pelo cálculo de rotas
(**DV**) Implementado no protocolo RIP
(**DV**) Troca de informações topológicas da rede e cálculo de rotas são etapas alternantes

---

Questão 4 ..... 20 pontos

Considere as seguintes informações criptográficas:

- K_A^+ e K_A^- o par de chaves pública e privada de Ana, respectivamente.
- K_B^+ e K_B^- o par de chaves pública e privada de Bruno, respectivamente.
- K_S uma chave simétrica de conhecimento exclusivo de Ana e de Bruno.
- $H(\cdot)$ uma função *hash* que gera um resumo de mensagem (*message digest*).
- M uma mensagem de texto qualquer.

Assuma que Ana e Bruno tenham conhecimento das respectivas chaves públicas do outro, e também conheçam a função $H(\cdot)$. Para cada afirmação a seguir, indique se a mesma é verdadeira ou falsa, e explique sua resposta utilizando *apenas uma frase*:

◯ Ao receber $K_S(H(M))$, Bruno é capaz de decifrar e ler a mensagem M transmitida por Ana.
O resumo gerado pela função $H(\cdot)$ não pode ser desfeito, ou seja, não pode ser invertido para obter a mensagem cifrada M.

√ $K_B^+(K_B^-(K_S(M))) = K_S(M)$
A chave pública aplicada a uma mensagem cifrada com a chave privada retorna a própria mensagem, que no caso é $K_S(M)$.

√ **Ao enviar $K_B^+(M)$ e $H(M)$ a Bruno, Ana garante confidencialidade e integridade ao envio da mensagem.**
Somente Bruno conhece sua chave privada K_B^-, logo somente ele é capaz de decifrar $K_B^+(M)$ e obter M; além disso, Bruno consegue detectar se $K_B^+(M)$ for modificada, pois a mensagem decriptada nesse caso terá um resumo diferente de $H(M)$.

◯ Bruno precisa conhecer K_A^- para verificar a autenticidade de uma mensagem M gerada por Ana.
Qualquer pessoa, não apenas Ana, conhece K_A^+ e pode gerar $K_A^-(M)$ a partir de M; para atribuir autenticidade a M, Ana precisa cifrá-la com sua chave privada K_A^-, logo Bruno precisa conhecer K_A^+.

√ **Ao receber $K_S(M)$, Bruno é capaz de concluir que M foi gerada por Ana.**
Apenas Ana e Bruno conhecem a chave simétrica K_S, logo Bruno sabe que apenas Ana pode ter gerado $K_S(M)$.

Questão 5 ..... 20 pontos

Considere um servidor realizando *streaming* de um vídeo para um cliente. Essa transmissão é composta de 24 pacotes numerados, enviados em slots de tempo pré-determinados (um pacote por slot).

Suponha também que, para cada grupo de 3 pacotes consecutivos, o servidor irá criar um pacote adicional FEC, contendo o XOR destes pacotes. Este pacote será incluído na transmissão, logo após o grupo correspondente, e sua transmissão irá ocupar um slot a mais. Caso o último grupo tenha menos que 3 pacotes, o último FEC será aplicado nos pacotes restantes.

(a) Qual é o objetivo da transmissão destes pacotes FEC?

Resposta:

O objetivo é permitir que pacotes que eventualmente sejam perdidos durante a transmissão possam ser recuperados sem que o cliente precise pedir que o servidor transmita-os novamente, pois este procedimento é muito demorado para reprodução de vídeo por *streaming*.

(b) Quantos pacotes (tanto vídeo como FEC) o servidor irá enviar ao cliente nesta transmissão?

Resposta:

Serão transmitidos 32 pacotes, sendo 24 pacotes de vídeo e 8 pacotes FEC.

(c) Suponha que, nos slots 1, 2, 16, 23, 24, 25, 29 e 30, os pacotes enviados se percam durante a transmissão (nos slots restantes, o pacote chega com sucesso). Quais pacotes de vídeo o cliente não irá receber?

Resposta:

O cliente não irá receber os pacotes de vídeo 1, 2, 18, 19, 22 e 23.

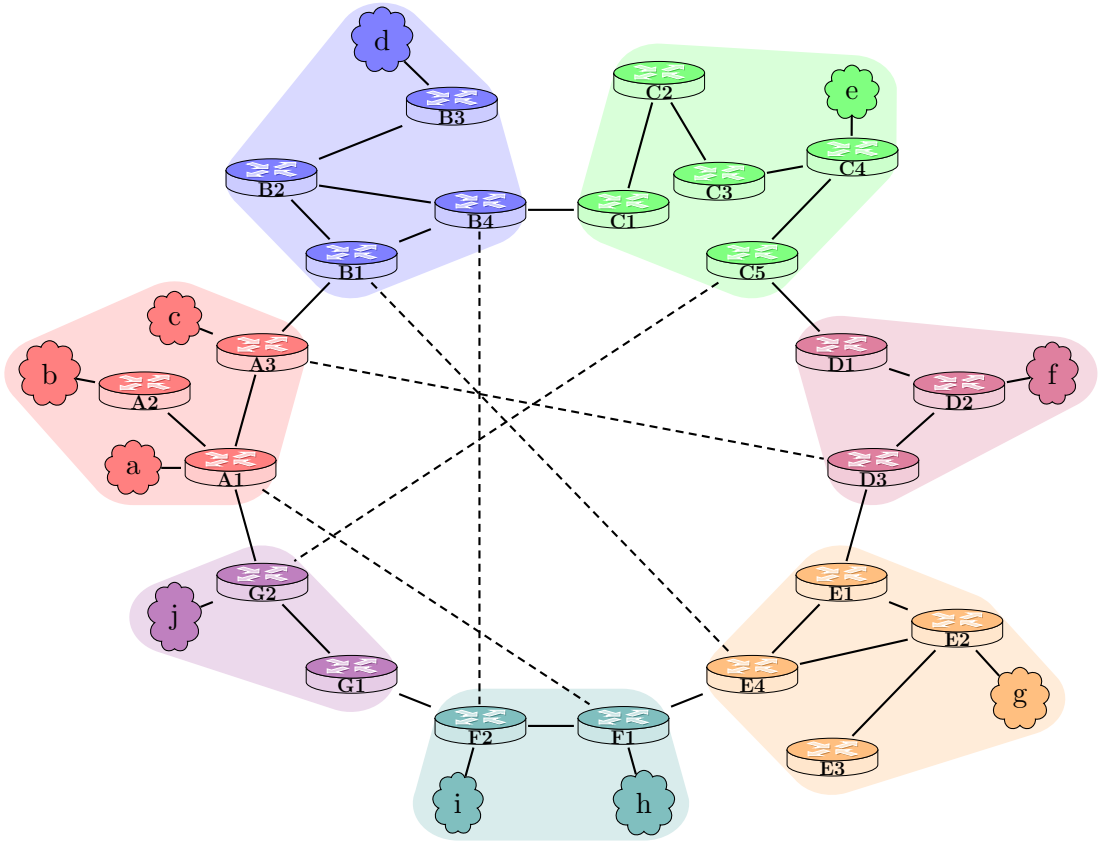
(d) No cenário descrito do item anterior, quais pacotes de vídeo o cliente não irá reproduzir?

Resposta:

Utilizando os pacotes FEC e os outros pacotes recebidos, o cliente somente será capaz de recuperar o pacote 19. Logo, ele não irá reproduzir os pacotes de vídeo 1, 2, 18, 22 e 23.

Questão 6 ..... 20 pontos

Na rede ilustrada a seguir, 7 sistemas autônomos, identificados por letras e cores distintas, encontram-se dispostos segundo um *backbone* circular, evidenciado pelos enlaces contínuos entre ASs. No entanto, devido à presença de tráfego intenso em rotas específicas, alguns ASs negociaram ligações diretas adicionais uns com os outros, representadas por linhas tracejadas, com uma condição de uso: cada enlace direto somente pode ser usado para tráfego direto entre os ASs em questão, sendo proibido o seu uso para trafegar dados de outros ASs. Não há restrições negociadas sobre o uso do *backbone*. Algumas das subredes presentes nestes ASs são ilustradas por letras minúsculas.



(a) Os roteadores F1 e A1 irão estabelecer alguma comunicação BGP um com o outro?

Se sim, do tipo iBGP ou eBGP?

Resposta:

Haverá comunicação eBGP entre estes roteadores.

(b) O AS D conhece uma rota até a subrede f, que está em seu domínio. Ele irá anunciar esta rota para o AS A? Por quê?

Resposta:

Sim, pois ao anunciar esta rota ao AS A através do enlace direto que os liga, ele está permitindo que A utilize este enlace para enviar pacotes com destino a D, o que satisfaz a restrição de uso do enlace.

(c) Considere um pacote enviado da subrede g para a subrede c. Determine o caminho que este pacote irá percorrer nesta rede, tanto em nível de sistemas autônomos quanto em nível de roteadores.

Resposta:

O pacote irá transitar através dos ASs E, F, G e A, sendo encaminhado pelos roteadores E2, E4, F1, F2, G1, G2, A1 e A3.