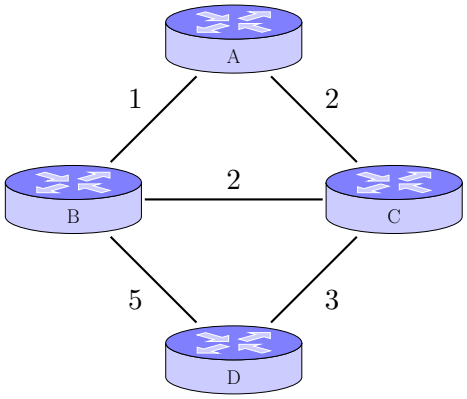
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP3 - 2º semestre de 2013 - GABARITO

Questão 1: [2.0 pontos] Considere as seguintes afirmações sobre protocolo IP e roteamento. Para cada afirmação, indique se a mesma é verdadeira ou falsa, e explique sua resposta utilizando *apenas uma frase*. Considere a rede da figura abaixo nas três primeiras afirmações.



1. Suponha que o nó A envie uma mensagem em broadcast usando o algoritmo de *flooding*. Esta mensagem será transmitida duas vezes somente no enlace B-C da rede, ou seja, de B para C e de C para B.

   Resposta: Falso. A mensagem também será transmitida duas vezes no enlace B-D, pois D receberá a mensagem de C antes de recebê-la de B e portanto a retransmitirá para B.

2. Suponha que o algoritmo de roteamento usado pelos nós seja o *link state routing*. Toda vez que houver uma atualização na tabela de roteamento do nó C, C enviará sua nova tabela para os seus vizinhos A, B e D.

   Resposta: Falso. No algoritmo link state routing, quando ocorre uma atualização na tabela de roteamento, nenhuma informação é enviada para os vizinhos.

3. Considere que o algoritmo de roteamento usado pelos nós é o vetor de distâncias. Toda vez que o nó D receber um novo vetor de distâncias de um de seus vizinhos B ou C, ele irá atualizar o seu vetor de distâncias.

   Resposta: Verdadeiro.

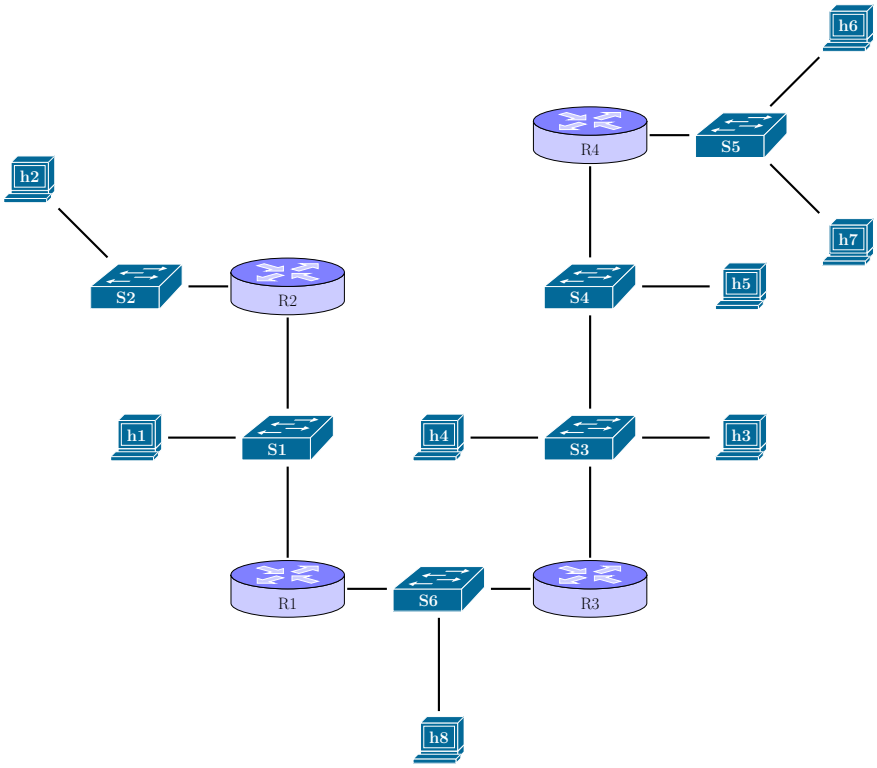
4. No protocolo IP, quando um datagrama precisa ser fragmentado, ele é remontado no próximo roteador para o qual é encaminhado.

Resposta: Falso. Quando um datagrama é fragmentado, ele é remontado na estação de destino.

5. O endereço IP 192.168.0.10 pode ser atribuído a uma máquina conectada a uma rede com máscara 255.255.255.0 e gateway 192.168.0.1.

Resposta: Verdadeiro.

Questão 2: [1.0 ponto] Considere a seguinte rede, composta de estações (h), switches (S) e roteadores (R):



Considere o seguinte cenário: h5 deseja enviar um pacote para h7, e para isto deve encapsular este pacote em um quadro. Enquanto isso, h3 deseja enviar um pacote para h5. Suponha que todas as tabelas ARP da rede estão vazias, e portanto, antes de encapsularem seus pacotes, ambas as estações transmissoras deverão enviar quadros *ARP query*.

- Qual o endereço MAC de destino destes quadros *ARP query*?

Resposta: Ambos os quadros serão enviados em broadcast e terão como MAC de destino o endereço MAC `ff:ff:ff:ff:ff:ff`, que é reservado para este propósito.

- Qual o endereço IP que estará contido nestes quadros?

Resposta: O quadro *ARP query* enviado por h5 conterá o endereço IP de R4, enquanto o enviado por h3 conterá o endereço IP de h5.

Questão 3: [2.0 pontos] Considere um conjunto de estações se comunicando por uma rede sem fio *ad hoc*. Considere que as estações não são terminais móveis e se encontram a uma determinada distância umas das outras conforme a tabela abaixo:

	A	B	C	D	E	F
A		3.3 m	6.9 m	7.1 m	5.6 m	3.3 m
B	3.3 m		3.9 m	6.8 m	7.0 m	6.4 m
C	6.9 m	3.9 m		6.3 m	8.4 m	9.4 m
D	7.1 m	6.8 m	6.3 m		3.6 m	7.2 m
E	5.6 m	7.0 m	8.4 m	3.6 m		4.1 m
F	3.3 m	6.4 m	9.4 m	7.2 m	4.1 m	

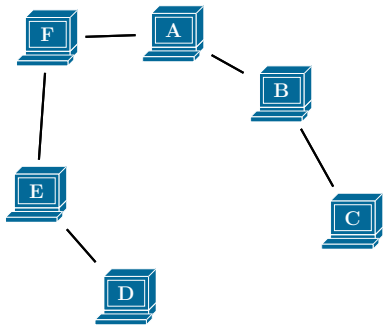
Suponha que duas estações conseguem se comunicar diretamente se, e somente se, elas encontram-se no máximo a uma distância de 5.5 m.

1. Esta restrição na comunicação é ocasionada por qual fenômeno observado em redes sem fio?

   Resposta: É ocasionada pelo *desvanecimento do sinal* em redes sem fio: ao contrário de redes cabeadas, em que o sinal é propagado por impulsos elétricos, em redes sem fio o meio de propagação das ondas de sinal causa uma grande queda na potência do sinal conforme ele se propaga.

2. O *grafo de conectividade* desta rede é um grafo no qual os vértices são as estações, e existe uma aresta entre duas estações se e somente se elas são capazes de ouvir a transmissão uma da outra. Construa o grafo de conectividade desta rede.

   Resposta:



3. Considere o cenário em que ocorrem simultaneamente transmissões de quadros de C para B e de A para F. As estações destino desses quadros irão receber os respectivos quadros com sucesso?

   Resposta: B não recebe a transmissão de C com sucesso pois recebe ambas as transmissões, o que significa que houve colisão. Já F recebe a transmissão de A com sucesso.

4. Repita o item anterior para o cenário em que ocorrem simultaneamente transmissões de quadros de E para D e de B para C.

   Resposta: D e C recebem suas transmissões com sucesso.

Questão 4: [1.0 ponto] Considere um mecanismo NAT cujo endereço IP na rede pública é 208.255.85.245 e que gerencia as conexões da rede privada, que ocupa a faixa 10.0.0.0/8. Suponha que o NAT possui a seguinte tabela de tradução de endereços:

(IP, porta) da estação local	(IP, porta) da estação remota	Porta pública no NAT
10.0.0.1, 10592	84.76.146.201, 24526	18388
10.0.0.2, 5625	5.166.174.58, 17281	24115
10.0.0.3, 3953	148.194.109.89, 15558	15754
10.0.0.3, 22326	105.148.199.30, 18505	1027
10.0.0.3, 24960	199.156.189.193, 18285	1024
10.0.0.1, 25613	4.184.163.251, 18533	21242
10.0.0.4, 32082	56.136.64.42, 10344	1029
10.0.0.3, 24236	149.144.162.79, 7706	22161
10.0.0.5, 25515	99.214.60.224, 26301	11605
10.0.0.2, 16258	212.167.221.135, 2239	24531

1. Considere os seguintes pacotes TCP que chegam ao NAT provenientes da rede pública (cuja estação de destino está na rede privada):

Pacote da rede pública:
FROM: 240.72.129.9, 3315 TO: 208.255.85.245, 1027
FROM: 84.76.146.201, 24526 TO: 208.255.85.245, 18388
FROM: 99.214.60.224, 26301 TO: 208.255.85.245, 1024

   Determine quais pacotes serão encaminhados para a rede privada com sucesso e, para estes pacotes, determine seu endereço e porta de origem e de destino após ele ser encaminhado à rede privada.

   Resposta:

Pacote da rede pública:	Pacote para a rede privada:
FROM: 240.72.129.9, 3315 TO: 208.255.85.245, 1027	descartado
FROM: 84.76.146.201, 24526 TO: 208.255.85.245, 18388	FROM: 84.76.146.201, 24526 TO: 10.0.0.1, 10592
FROM: 99.214.60.224, 26301 TO: 208.255.85.245, 1024	descartado

2. Considere agora os seguintes pacotes TCP que chegam ao NAT provenientes da rede privada (cuja estação de destino está na rede pública):

Pacote da rede privada:
FROM: 10.0.0.4, 32082 TO: 245.2.225.178, 8424
FROM: 10.0.0.3, 22326 TO: 105.148.199.30, 18505
FROM: 10.0.0.2, 5625 TO: 5.166.174.58, 17281

   Determine quais destes pacotes levarão à criação de novas entradas na tabela de tradução. Determine também os endereços e portas, de origem e de destino, de todos os pacotes após eles serem encaminhados à rede pública.

Resposta:

Pacote da rede privada:	Pacote para a rede pública:	Nova entrada?
FROM: 10.0.0.4, 32082 TO: 245.2.225.178, 8424	FROM: 208.255.85.245, 1025 TO: 245.2.225.178, 8424	✓
FROM: 10.0.0.3, 22326 TO: 105.148.199.30, 18505	FROM: 208.255.85.245, 1027 TO: 105.148.199.30, 18505	
FROM: 10.0.0.2, 5625 TO: 5.166.174.58, 17281	FROM: 208.255.85.245, 24115 TO: 5.166.174.58, 17281	

Questão 5: [2.0 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 de *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 $H(\cdot)$.

Responda às perguntas abaixo de forma discursiva mas objetiva, focando apenas no que está sendo solicitado.

1. É possível que Ana envie uma mensagem a Bruno que seja confidencial mas que não seja autenticada? Caso positivo, dê um exemplo utilizando as informações criptográficas acima.

   Resposta: Sim, pois confidencialidade e autenticidade são duas propriedades distintas de uma comunicação com segurança em rede. Por exemplo, Ana pode enviar a Bruno $K_B^+(M)$ o que faz que com a mensagem M seja confidencial, ou seja, somente Bruno pode ler a mensagem utilizando sua chave privada. Entretanto, Bruno não tem como verificar a autenticidade de M pois qualquer outra pessoa pode ter escrito e transmitido M se passando por Ana.

2. Explique porque a função de *hash* $H(\cdot)$ utilizada para gerar resumos de mensagens não pode ser facilmente invertida. Ilustre o problema que teríamos neste caso utilizando as informações criptográficas acima.

   Resposta: Se a função de *hash* $H(\cdot)$ for fácil de inverter, então dado o resumo $H(M)$ poderíamos facilmente encontrar outras mensagens $M_1, M_2, M_3, \ldots$, cujos resumos são iguais ao de M, ou seja, $H(M_i) = H(M)$, para $i = 1, 2, 3, \ldots$. Com isto poderíamos falsificar a assinatura digital de forma que não possa ser detectado. Por exemplo, imagine que Ana assine o resumo da mensagem M, com o objetivo de autenticar M. Ou seja, Ana produz $K_A^-(H(M))$. Com isto qualquer um pode obter $H(M)$, e caso seja fácil de inverter, podemos obter M_1 tal que $H(M_1) = H(M)$. Desta forma, $K_A^-(H(M))$ também é assinatura digital para M_1, apesar de Ana nunca ter autenticado M_1!

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

3. Ao receber $K_S(M)$ de Ana, Bruno é capaz de decifrar e ler a mensagem M transmitida por Ana.

> **Resposta:** Verdadeiro. Bruno possui a chave simétrica K_S que é usada tanto para cifrar quanto para decifrar uma mensagem, ou seja, $K_S(K_S(M)) = M$

4. Ao receber $H(M)$ de Ana, Bruno é capaz de decifrar e ler a mensagem M transmitida por Ana.

> **Resposta:** Falso. Ao receber o resumo da mensagem $H(M)$, Bruno não é capaz de reconstruir M uma vez que $H(\text{cot})$ não é facilmente inversível (e mesmo que fosse ele não saberia qual M foi transmitida por Ana).

5. $K_B^+(K_B^-(K_S(M))) = M$

> **Resposta:** Falso. A chave pública aplicada à chave privada retorna o valor do argumento interno, ou seja, $K_B^+(K_B^-(K_S(M))) = K_S(M)$.

Questão 6: [2.0 pontos] Considere duas estações compartilhando um meio de transmissão com largura de banda igual a 500 Mbps. A estação 1 deseja transmitir 375000 bytes de dados a partir do instante t = 60 ms, enquanto a estação 2 deseja transmitir 187500 bytes a partir de t = 80 ms.

1. Considere que o controle de acesso seja feito através do protocolo TDMA, com slots de 20 ms, a iniciar pela estação 1. Suponha que não haja atraso de propagação entre as estações. Em que instantes de tempo cada uma das estações irá iniciar e terminar sua transmissão? Haverá colisão entre as transmissões?

> **Resposta:** A estação 1 transmite entre t = 80 ms e t = 180 ms, e a estação 2 transmite entre t = 100 ms e t = 150 ms. Como cada estação só transmite em seus respectivos slots, não há colisão.

2. Considere agora que o controle de acesso seja feito através do protocolo CSMA. Suponha que entre as estações existe um atraso de propagação igual a 30 ms. Em que instantes de tempo as estações começam e terminam de transmitir? Haverá colisão?

> **Resposta:** A estação 1 transmite entre t = 60 ms e t = 120 ms, e a estação 2 transmite entre t = 80 ms e t = 110 ms. Haverá colisão entre as transmissões.