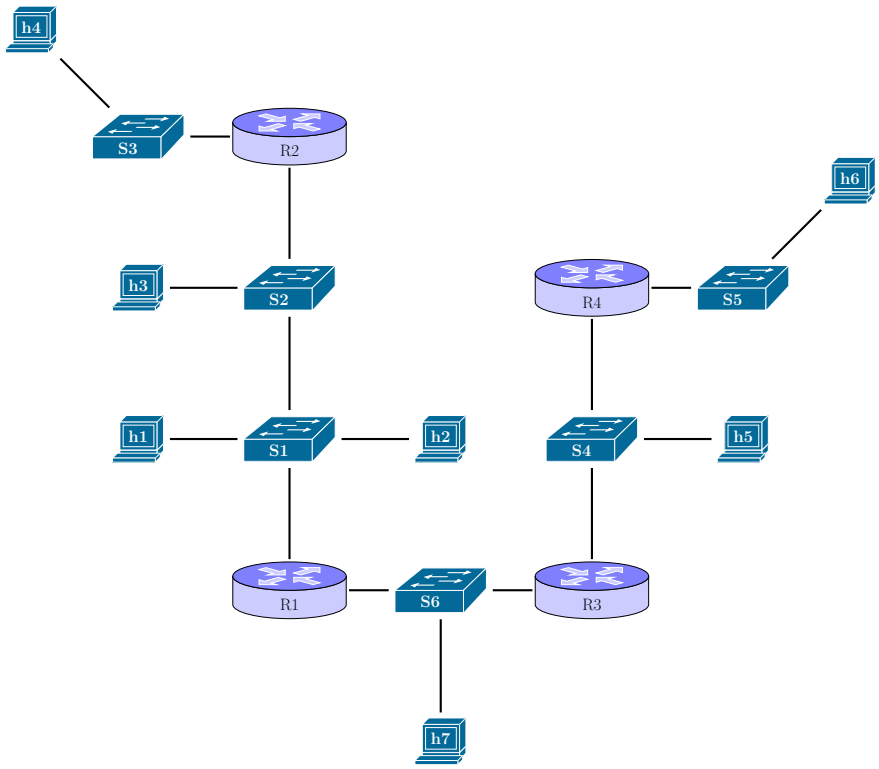
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 – 1º semestre de 2014 – GABARITO

Questão 1 ..... 15 pontos

Considere a seguinte rede, composta de estações (h), switches (S) e roteadores (R):



Considere o cenário em que h4 deseja enviar um pacote para h6 e, para isto deve encapsular este pacote em um quadro. Suponha que todas as tabelas ARP da rede estão vazias, e portanto, antes de encapsular seu pacote, h4 deve enviar um quadro *ARP query*.

(a) Qual o endereço MAC de destino deste ARP query?

Resposta:

O quadro será enviado em broadcast, logo terá como MAC de destino o endereço MAC `ff:ff:ff:ff:ff:ff`, que é reservado para este propósito.

(b) Qual o endereço IP que estará contido neste quadro?

Resposta:

O quadro conterá o endereço IP de R2.

(c) A estação h7 irá receber este ARP query? Por que?

Resposta:

Não, pois h7 e h4 estão em redes locais diferentes.

Questão 2 ..... 20 pontos

Considere o problema de autenticação em redes de computadores no qual Ana deseja provar sua identidade para Bruno na presença de Carla, que tem poderes para capturar e modificar mensagens que trafegam pela rede. Assuma que Ana e Bruno compartilham um segredo, ou seja, uma chave simétrica, K_S, que será utilizada pelo algoritmo de autenticação. Para cada afirmação abaixo, indique se a mesma é verdadeira ou falsa, e explique sua resposta utilizando *apenas uma frase*.

◯ Para se autenticar, é necessário que Ana gere um *nonce* (número nunca antes utilizado), cifre-o utilizando a chave K_S, e envie o resultado a Bruno.
Para que Ana se autentique para Bruno, Bruno deve gerar um *nonce* e enviá-lo a Ana em texto aberto (não cifrado), para que Ana cifre o *nonce* utilizando a chave K_S, e envie o resultado a Bruno.

◯ Carla consegue se passar por Ana se ela obtiver o valor do *nonce* (número nunca antes utilizado) que será utilizado durante uma determinada autenticação.
Mesmo que Carla conheça o valor do *nonce*, ela não sabe como cifrá-lo pois Carla desconhece a chave K_S, impedindo assim sua autenticação.

Considere o ataque conhecido por homem-no-meio (*man-in-the-middle attack*) onde Carla consegue interceptar e ter acesso às mensagens cifradas sendo trocadas por Ana e Bruno. Para cada afirmação abaixo, indique se a mesma é verdadeira ou falsa, e explique sua resposta utilizando *apenas uma frase*.

√ **O ataque homem-no-meio pode ocorrer apenas quando Ana e Bruno utilizam o sistema de criptografia baseado em chave pública-privado.**
Este ataque só é possível no contexto de criptografia baseada em chave pública-privado, quando as duas partes envolvidas na autenticação precisam trocar suas chaves públicas.

√ **O ataque homem-no-meio nunca pode ocorrer se Ana e Bruno tem conhecimento prévio das respectivas chaves públicas do outro.**
Para que o ataque possa ocorrer é necessário que Ana e Bruno enviem um ao outro suas respectivas chaves públicas, o que só é necessário se eles não possuem conhecimento prévio destas chaves.

Questão 3 ..... 25 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 distância fixa umas das outras conforme a tabela abaixo:

	A	B	C	D	E	F	G	H	I
A		2.9 m	6.1 m	6.3 m	8.4 m	8.7 m	6.8 m	6.4 m	4.3 m
B	2.9 m		3.4 m	4.5 m	8.0 m	9.3 m	8.1 m	8.9 m	7.1 m
C	6.1 m	3.4 m		2.9 m	7.3 m	9.7 m	9.4 m	11.4 m	10.3 m
D	6.3 m	4.5 m	2.9 m		4.4 m	7.0 m	7.2 m	10.0 m	10.0 m
E	8.4 m	8.0 m	7.3 m	4.4 m		3.2 m	4.8 m	8.8 m	10.6 m
F	8.7 m	9.3 m	9.7 m	7.0 m	3.2 m		2.7 m	6.8 m	9.5 m
G	6.8 m	8.1 m	9.4 m	7.2 m	4.8 m	2.7 m		4.2 m	6.9 m
H	6.4 m	8.9 m	11.4 m	10.0 m	8.8 m	6.8 m	4.2 m		4.0 m
I	4.3 m	7.1 m	10.3 m	10.0 m	10.6 m	9.5 m	6.9 m	4.0 m	

Suponha que duas estações conseguem se comunicar diretamente se, e somente se, elas encontram-se no máximo a uma distância de 6.0 m.

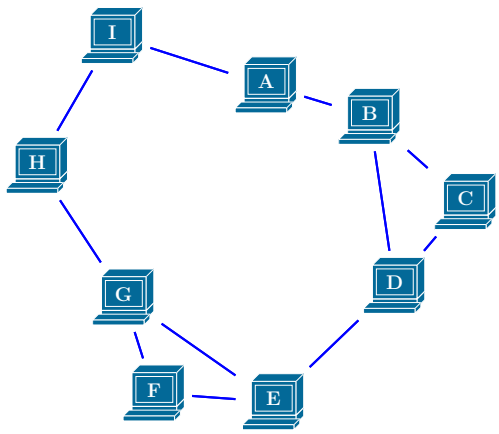
(a) Esta restrição na comunicação é ocasionada por qual fenômeno observado em redes sem fio? Explique como ele ocorre.

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.

(b) 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:



(c) Considere o cenário em que ocorrem simultaneamente transmissões de quadros de A para B e de D para E. As estações destino desses quadros irão receber os respectivos quadros com sucesso?

Resposta:

B não recebe a transmissão de A com sucesso pois recebe ambas as transmissões, o que significa que houve colisão. Já E recebe a transmissão de D com sucesso.

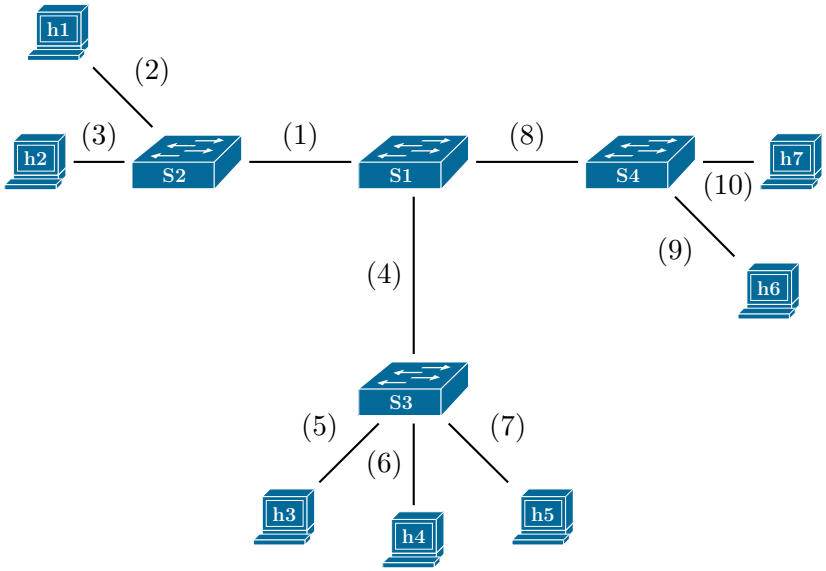
(d) Repita o item anterior para o cenário em que ocorrem simultaneamente transmissões de quadros de C para D e de F para E.

Resposta:

D e E recebem suas transmissões com sucesso.

Questão 4 ..... 10 pontos

Considere a rede local de uma empresa, estruturada conforme a seguinte topologia:



Os números entre parênteses são os identificadores de cada enlace. Considere que, em um dado momento, as tabelas de encaminhamento dos switches sejam as seguintes:

Tabela de S1	
Destino	Interface
h6	8
h2	1
h1	1
h7	8
h4	4

Tabela de S2	
Destino	Interface
h6	1
h2	3
h1	2
h7	1

Tabela de S3	
Destino	Interface
h6	4
h1	4
h4	6

Tabela de S4	
Destino	Interface
h6	9
h2	8
h1	8
h7	10
h4	8

(a) Se a estação h2 enviar um quadro para a estação h5, por quais enlaces esse quadro será transmitido?

Resposta:

O quadro será transmitido pelos enlaces 1, 2, 3, 4, 5, 6, 7, 8, 9 e 10.

(b) Durante a transmissão deste quadro, algum dos switches desta rede irá adicionar alguma entrada em sua tabela de encaminhamento? Se sim, quais switches e quais entradas?

Resposta:

Os seguintes switches irão adicionar entradas em sua tabela de encaminhamento:

- Switch S3 — destino h2 / interface 4

Questão 5 ..... 20 pontos

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

◯ 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.

√ **Se o retardo fim-a-fim entre um usuário A e um usuário B é constante então o jitter é igual a zero.**
O jitter é a variação do retardo fim-a-fim entre os pacotes transmtidos de um usuário A para um usuário B. Portanto se o retardo fim-a-fim é constante, não existe variação e o jitter é zero.

◯ 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 serão 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.

√ **Um pacote de uma aplicação multimídia 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.

Questão 6 ..... 10 pontos

Considere uma rede sem fio formada por três estações (ex. três notebooks) denominados A, B, e C. Faça um desenho do grafo de conectividade (vértices são estações e arestas indicam que um par de estações é capaz de trocar mensagens) que caracterize o problema do terminal escondido. Utilizando sua figura, indique qual estação está escondida de qual.

Resposta:

O grafo de conectividade que caracteriza este problema é X —— Y —— Z, onde X, Y e Z podem corresponder a qualquer permutação das estações A, B e C (por exemplo, X=A, Y=B, Z=C). Nesta rede, as estações X e Z não podem trocar mensagens (estão fora do raio de comunicação), e por isto estão escondidas uma da outra. Por outro lado, a estação Y não está escondida de nenhuma outra, uma vez que esta pode trocar mensagens com as outras. Logo, X e Z podem transmitir ao mesmo tempo para Y sem escutar a outra transmissão e, portanto, sem detectar a colisão.