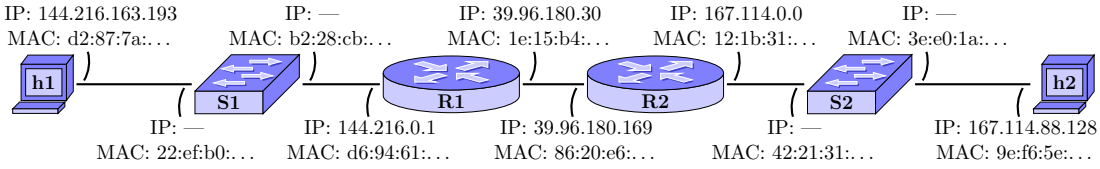
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 – 1º semestre de 2015 – GABARITO

Questão 1 ..... 20 pontos

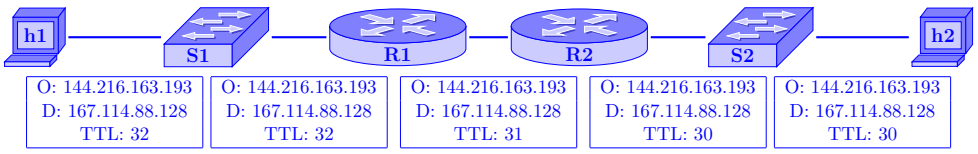
Considere a rede ilustrada a seguir, composta por duas estações (h1 e h2), dois switches (S1 e S2) e dois roteadores (R1 e R2). Suponha, para simplificar, que o protocolo Ethernet é utilizado em todas as comunicações na camada de enlace. No diagrama, são associados a cada interface os seus respectivos endereços IP e MAC (para o endereço MAC, somente os primeiros octetos).



Considere um datagrama IP que é enviado de h1 com destino a h2.

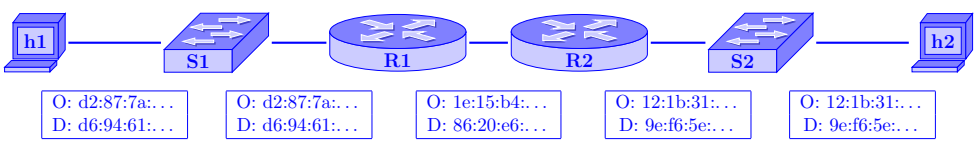
(a) Lembrando que o campo TTL (*Time to Live*) do cabeçalho IP é diminuído de uma unidade a cada salto, suponha que o datagrama é enviado com TTL inicial de 32. Para cada um dos 5 enlaces que o datagrama irá atravessar, determine o endereço origem, o endereço destino e o valor de TTL registrados no cabeçalho deste datagrama quando ele atravessa o enlace.

Resposta:



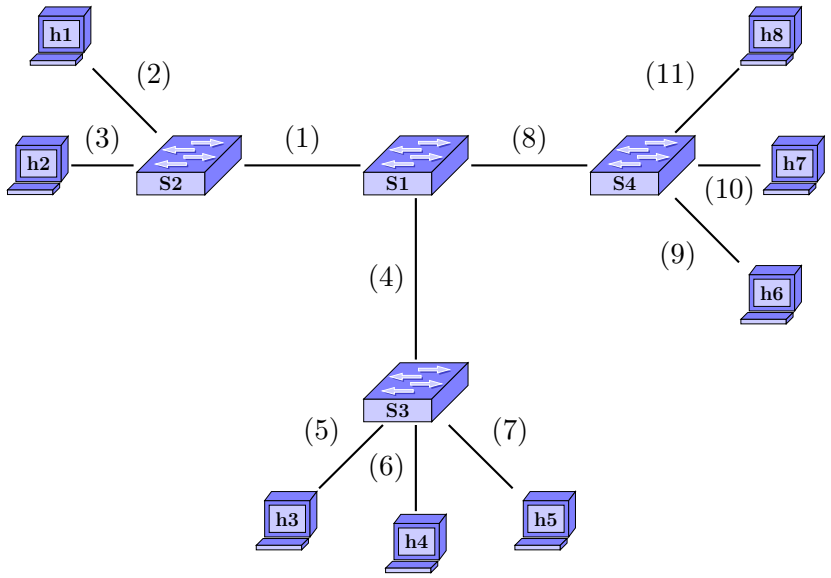
(b) Suponha que todas as tabelas ARP envolvidas estão devidamente preenchidas. Para cada um dos 5 enlaces, determine o endereço origem e o endereço destino dos quadros Ethernet que irão encapsular este datagrama quando ele atravessa o enlace.

Resposta:



Questão 2 ..... 20 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
h8	8
h7	8
h3	4
h4	4

Tabela de S2	
Destino	Interface
h8	1
h7	1
h4	1

Tabela de S3	
Destino	Interface
h8	4
h7	4
h3	5
h4	6

Tabela de S4	
Destino	Interface
h8	11
h7	10
h3	8
h4	8

(a) Se a estação h2 enviar um quadro para a estação h3, por quais enlaces esse quadro será transmitido?

Resposta:

O quadro será transmitido pelos enlaces 1, 2, 3, 4 e 5.

(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 S1 — destino h2 / interface 1
- Switch S2 — destino h2 / interface 3
- Switch S3 — destino h2 / interface 4

Questão 3 ..... 25 pontos

Um dos protocolos mais utilizados na Internet para prover segurança na comunicação entre duas entidades é o *Transport Layer Security*, ou TLS. Este protocolo pode ser utilizado em conjunto com qualquer protocolo de comunicação da camada de aplicação. Uma versão

simplificada do TLS é descrita no passo-a-passo a seguir, para uma comunicação entre um cliente e um servidor:

1. O cliente inicia o protocolo solicitando ao servidor o início de uma comunicação segura;
2. O servidor envia ao cliente seu certificado digital (que inclui a chave pública do servidor, que chamaremos de K_A^+) e um *nonce* n_1;
3. O cliente valida o certificado digital do servidor em uma entidade certificadora (se a validação falhar, o cliente encerra a comunicação);
4. O cliente gera um segundo *nonce* n_2, cifra-o com a chave K_A^+, e o envia de volta ao servidor;
5. Utilizando ambos os *nonce*'s (e apenas eles), o cliente e o servidor geram uma chave simétrica, que chamaremos de K_S. O mesmo algoritmo é utilizado pelo cliente e pelo servidor para gerar a chave, e é definido na especificação do protocolo TLS;

Este passo-a-passo descreve o *handshake TLS*. Após o handshake, o cliente e o servidor passam a realizar a comunicação original que desejavam, mas sempre cifrando as mensagens com a chave simétrica K_S antes de enviá-las e decifrando-as com a mesma chave ao recebê-las.

Determine se cada uma das afirmações a seguir é verdadeira ou falsa e justifique usando *apenas uma frase*. Para cada uma delas, salvo em afirmação contrária, suponha que as chaves privadas envolvidas não são conhecidas, nem o servidor nem o cliente geram *nonce*'s duplicados, e a entidade certificadora envolvida é confiável.

√ **Um atacante que tenha acesso a todas as mensagens trocadas no handshake e obtenha o valor de n_2 é capaz de decriptar todas as mensagens enviadas após o handshake.**
De posse de n_1 (que foi enviado abertamente na rede) e n_2, o atacante é capaz de gerar K_S utilizando o mesmo algoritmo executado pelo cliente e pelo servidor (que é publicamente conhecido).

◯ Este protocolo garante ao servidor a autenticidade do cliente.
O cliente não envia nenhuma informação que só ele próprio poderia saber, logo é possível que um atacante finja ser o cliente e se comunique com o servidor sem ser detectado.

√ **Um atacante que tenha acesso a todas as mensagens trocadas no handshake é incapaz de obter o valor de n_2.**
Como somente $K_A^+(n_2)$ circula na rede, o atacante deveria conhecer a chave privada do servidor (K_A^-) para obter n_2.

√ **Este protocolo garante a confidencialidade da comunicação após o handshake.**
Somente o cliente e o servidor conhecem a chave K_S, e é impossível ter acesso aos dados cifrados sem conhecer esta chave.

◯ O uso dos *nonce*'s n_1 e n_2 impede que um atacante com a habilidade de de modificar as mensagens realize um ataque do homem-no-meio sobre o handshake.
Neste ataque, o intruso deverá substituir a chave pública do servidor (K_A^+) pela sua própria chave pública, o que será detectado pelo cliente, pois a entidade certificadora irá rejeitar sua tentativa de validação do certificado, mesmo com o uso dos *nonce*'s.

Questão 4 ..... 15 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
A		5.0 m	7.8 m	9.5 m	8.2 m	7.1 m	2.9 m
B	5.0 m		3.7 m	6.7 m	7.2 m	8.9 m	6.2 m
C	7.8 m	3.7 m		3.4 m	5.2 m	8.5 m	7.7 m
D	9.5 m	6.7 m	3.4 m		3.1 m	7.3 m	8.3 m
E	8.2 m	7.2 m	5.2 m	3.1 m		4.3 m	6.3 m
F	7.1 m	8.9 m	8.5 m	7.3 m	4.3 m		4.3 m
G	2.9 m	6.2 m	7.7 m	8.3 m	6.3 m	4.3 m	

Suponha que duas estações conseguem se comunicar diretamente se, e somente se, elas encontram-se no máximo a uma distância de 6.8 m.

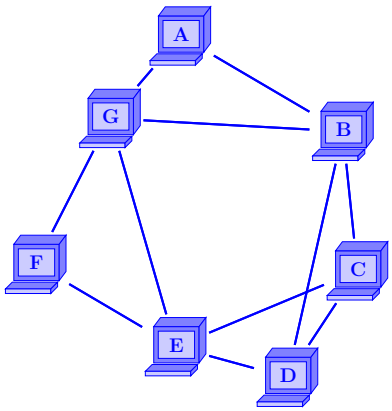
(a) Esta restrição na comunicação é ocasionada por qual fenômeno observado em redes sem fio? Explique como ele ocorre.

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 B para G e de D para E. As estações destino desses quadros irão receber os respectivos quadros com sucesso?

Resposta:

G e E recebem suas transmissões com sucesso.

(d) Repita o item anterior para o cenário em que ocorrem simultaneamente transmissões

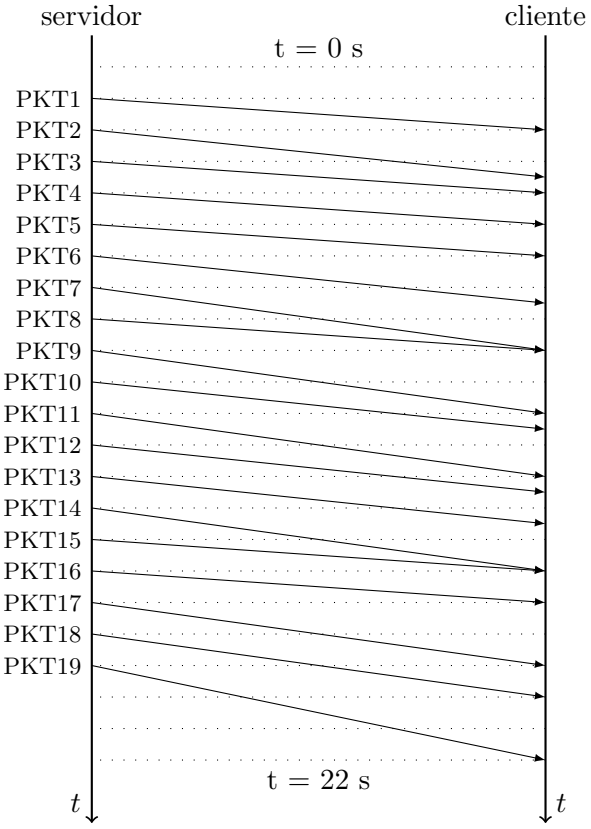
de quadros de G para E e de D para B.

Resposta:

Tanto E quanto B recebem ambas as transmissões, ocasionando colisão. Logo, nenhuma das transmissões é recebida com sucesso.

Questão 5 ..... 20 pontos

Considere a transmissão em *streaming* de pacotes multimídia de um servidor para um cliente, ilustrada no seguinte diagrama:



Suponha que o cliente utilize o seguinte mecanismo de bufferização: todos os pacotes são bufferizados assim que chegam e o cliente começa a reproduzir o vídeo somente ao receber o 1º pacote, considerando como perdidos todos os pacotes que não chegarem a tempo de serem reproduzidos.

(a) Determine o instante de recepção de cada um dos pacotes.

(b) Determine o instante de reprodução escalonado para cada um dos pacotes.

Resposta:

PKT1 Recepção em t = 2.0 s, reprodução escalonada para t = 2.0 s
PKT2 Recepção em t = 3.5 s, reprodução escalonada para t = 3.0 s
PKT3 Recepção em t = 4.0 s, reprodução escalonada para t = 4.0 s
PKT4 Recepção em t = 5.0 s, reprodução escalonada para t = 5.0 s
PKT5 Recepção em t = 6.0 s, reprodução escalonada para t = 6.0 s
PKT6 Recepção em t = 7.5 s, reprodução escalonada para t = 7.0 s
PKT7 Recepção em t = 9.0 s, reprodução escalonada para t = 8.0 s
PKT8 Recepção em t = 9.0 s, reprodução escalonada para t = 9.0 s
PKT9 Recepção em t = 11.0 s, reprodução escalonada para t = 10.0 s
PKT10 Recepção em t = 11.5 s, reprodução escalonada para t = 11.0 s
PKT11 Recepção em t = 13.0 s, reprodução escalonada para t = 12.0 s
PKT12 Recepção em t = 13.5 s, reprodução escalonada para t = 13.0 s
PKT13 Recepção em t = 14.5 s, reprodução escalonada para t = 14.0 s
PKT14 Recepção em t = 16.0 s, reprodução escalonada para t = 15.0 s
PKT15 Recepção em t = 16.0 s, reprodução escalonada para t = 16.0 s
PKT16 Recepção em t = 17.0 s, reprodução escalonada para t = 17.0 s
PKT17 Recepção em t = 19.0 s, reprodução escalonada para t = 18.0 s
PKT18 Recepção em t = 20.0 s, reprodução escalonada para t = 19.0 s
PKT19 Recepção em t = 22.0 s, reprodução escalonada para t = 20.0 s

(c) Algum pacote não será reproduzido com sucesso? Se sim, determine quais.

Resposta:

Sim, os pacotes 2, 6, 7, 9, 10, 11, 12, 13, 14, 17, 18 e 19 não serão reproduzidos com sucesso.

(d) Calcule a fração de pacotes perdidos para esta transmissão.

Resposta:

A fração de pacotes perdidos é dada pela quantidade de pacotes perdidos, dividida pelo total de pacotes transmitidos, resultando em uma perda de 12/19 = 63.2%.