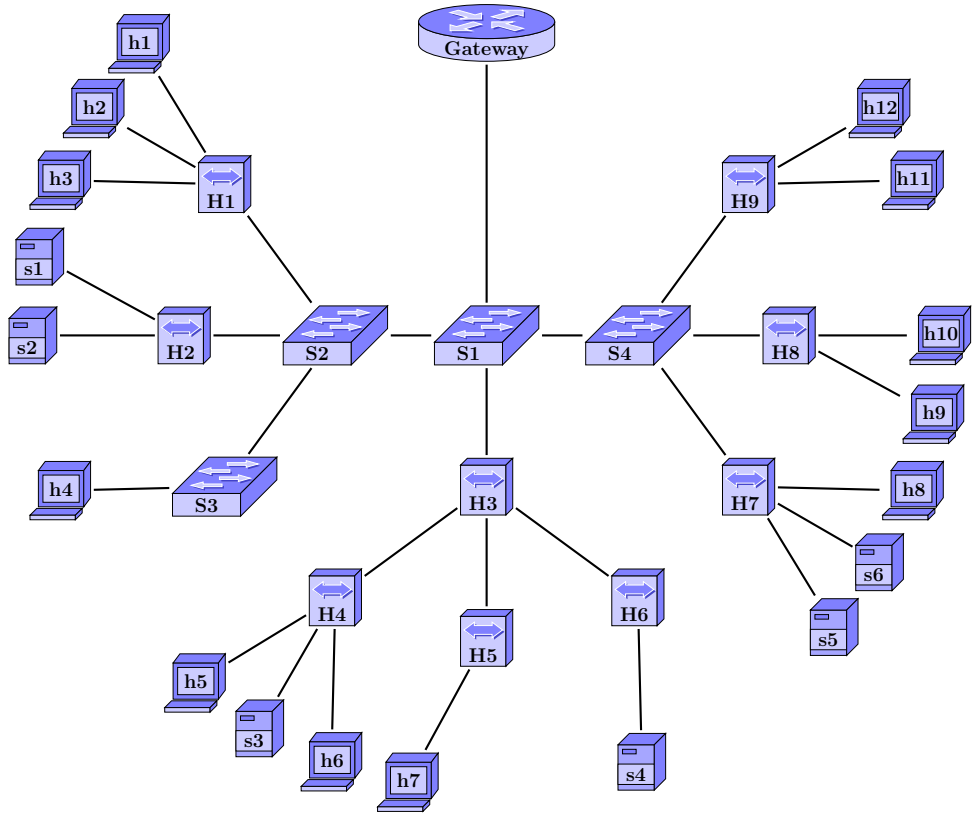
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 – 2º semestre de 2020 – GABARITO

Questão 1 ..... 20 pontos

Considere a seguinte rede local, formada por estações (indicadas pela letra h), servidores (s), hubs (H) e switches (S), cuja saída para a Internet se dá através de um único gateway.



(a) Suponha que ocorre a transmissão de um fluxo de quadros de s6 para h5. Por quais equipamentos (estações, servidores, hubs e switches) esse fluxo irá transitar?

Resposta:

A transmissão será vista por h5, h6, h7, h8, H3, H4, H5, H6, H7, s3, s4, s5, s6, S1 e S4.

(b) Considere que todos os servidores e estações possuem dados a transmitir para a Inter-

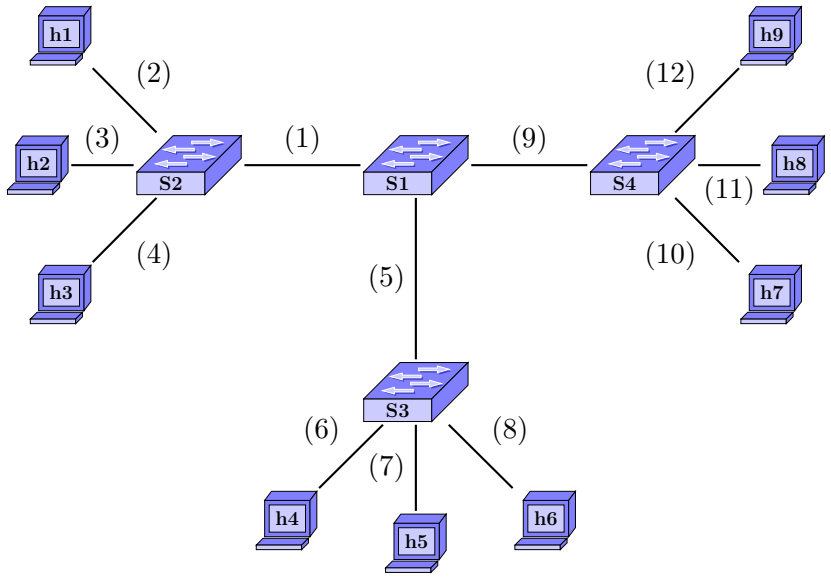
net. Qual o número máximo destes equipamentos que podem realizar essa transmissão simultaneamente, sem que ocorram colisões? Descreva um cenário em que este máximo é atingido.

Resposta:

Pode haver no máximo 7 transmissões simultâneas para a Internet, sem que haja colisão. Este máximo é atingido, por exemplo, com transmissões de h1, h4, h5, h9, h11, s1 e s5.

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
h6	5
h7	9

Tabela de S2	
Destino	Interface
h6	1
h7	1

Tabela de S3	
Destino	Interface
h6	8
h4	6
h7	5

Tabela de S4	
Destino	Interface
h6	9
h7	10

(a) Se a estação h3 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, 10, 11 e 12.

(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?

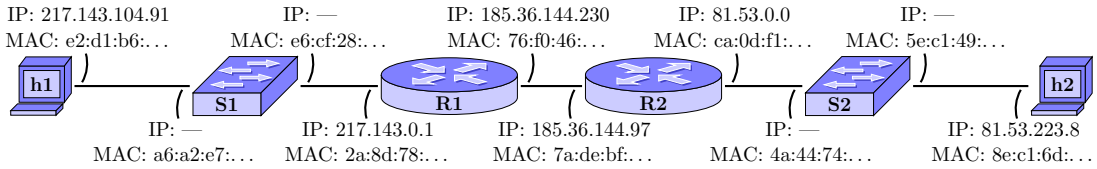
Resposta:

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

- Switch S1 — destino h3 / interface 1
- Switch S2 — destino h3 / interface 4
- Switch S3 — destino h3 / interface 5
- Switch S4 — destino h3 / interface 9

Questão 3 ..... 20 pontos

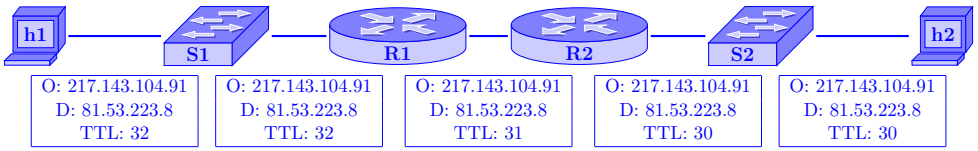
Considere a rede ilustrada a seguir, composta por duas estações (h1 e h2), dois switches (S1 e S2) e dois roteadores (R1 e R2). Suponha, para simplificar, que o protocolo Ethernet é utilizado em todas as comunicações na camada de enlace. No diagrama, são associados a cada interface os seus respectivos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

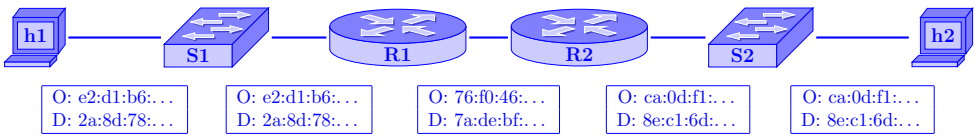
(a) Lembrando que o campo TTL (*Time to Live*) do cabeçalho IP é diminuído de uma unidade a cada salto, suponha que o datagrama é enviado com TTL inicial de 32. Para cada um dos 5 enlaces que o datagrama irá atravessar, determine o endereço origem, o endereço destino e o valor de TTL registrados no cabeçalho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

Resposta:



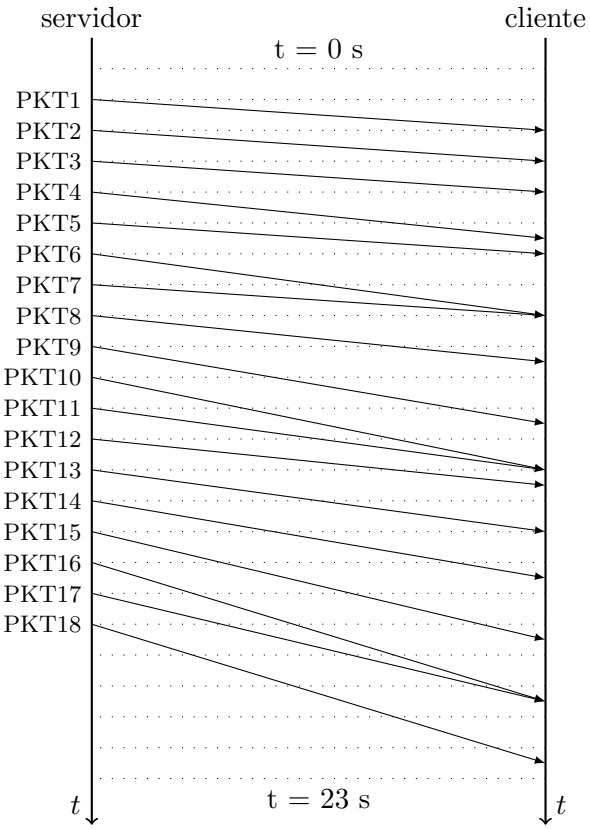
(b) Suponha que todas as tabelas ARP envolvidas estão devidamente preenchidas. Para cada um dos 5 enlaces, determine o endereço origem e o endereço destino dos quadros Ethernet que irão encapsular este datagrama quando ele atravessa o enlace.

Resposta:



Questão 4 ..... 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 2.0 s após o primeiro pacote chegar, 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 = 4.0 s
PKT2 Recepção em t = 3.0 s, reprodução escalonada para t = 5.0 s
PKT3 Recepção em t = 4.0 s, reprodução escalonada para t = 6.0 s
PKT4 Recepção em t = 5.5 s, reprodução escalonada para t = 7.0 s
PKT5 Recepção em t = 6.0 s, reprodução escalonada para t = 8.0 s
PKT6 Recepção em t = 8.0 s, reprodução escalonada para t = 9.0 s
PKT7 Recepção em t = 8.0 s, reprodução escalonada para t = 10.0 s
PKT8 Recepção em t = 9.5 s, reprodução escalonada para t = 11.0 s
PKT9 Recepção em t = 11.5 s, reprodução escalonada para t = 12.0 s
PKT10 Recepção em t = 13.0 s, reprodução escalonada para t = 13.0 s
PKT11 Recepção em t = 13.0 s, reprodução escalonada para t = 14.0 s
PKT12 Recepção em t = 13.5 s, reprodução escalonada para t = 15.0 s
PKT13 Recepção em t = 15.0 s, reprodução escalonada para t = 16.0 s
PKT14 Recepção em t = 16.5 s, reprodução escalonada para t = 17.0 s
PKT15 Recepção em t = 18.5 s, reprodução escalonada para t = 18.0 s
PKT16 Recepção em t = 20.5 s, reprodução escalonada para t = 19.0 s
PKT17 Recepção em t = 20.5 s, reprodução escalonada para t = 20.0 s
PKT18 Recepção em t = 22.5 s, reprodução escalonada para t = 21.0 s

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

Resposta:

Sim, os pacotes 15, 16, 17 e 18 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 4/18 = 22.2%.

Questão 5 ..... 20 pontos

O objetivo desta questão é compreender o funcionamento de algoritmos geradores de resumo de mensagem (*message digest*). Em particular, iremos focar nos padrões MD5 e SHA1, que são dois padrões muito conhecidos e utilizados para funções de hash $H(\cdot)$, que geram resumo de mensagem — isto é, dada uma mensagem M qualquer, cada um destes padrões gera um resumo. Este resumo pode ser utilizado para diversos fins, desde alocação eficiente em estruturas de dados até verificação de integridade de mensagens transmitidas em uma rede.

(a) Qual é o tamanho do resumo (em bits) gerado pelos padrões MD5 e SHA1? Este tamanho depende do tamanho da mensagem M?

Resposta:

O MD5 sempre gera resumos de 128 bits e o SHA1 sempre gera resumos de 160 bits. Estes tamanhos de resumo não dependem do tamanho de M.

(b) Qual é o tamanho mínimo que M deve ter (em bytes) para que as funções de hash

MD5 e SHA1 possam ser utilizadas?

Resposta:

As funções de hash MD5 e SHA1 não determinam um tamanho mínimo para M. Logo, M pode ter qualquer tamanho.

(c) Determine o resumo da seguinte mensagem (sem aspas) quando utilizamos o padrão MD5 e o padrão SHA1: "Boas funções de hash são sensíveis a modificações!"[1] Apresente o resumo em formato hexadecimal.

Resposta:

O resumo MD5 desta frase é "`c82c8346c80c938fd2cc6a8a53033669`", e o seu resumo SHA1 é "`e5c0ca4f6a30d97f925645758a63c1e611cd9ea7`".

(d) Repita o item anterior para a seguinte mensagem (sem aspas): "Boas funções de hash são sensíveis a modificações." Repare que apenas um caractere foi trocado (ponto de exclamação para ponto final).

Resposta:

O resumo desta frase (com ponto final) utilizando a função de hash MD5 é "`a48d2299b9f26ff6d7d63f42108f9c01`", e utilizando o SHA1 é "`8a4fbf99ee7df1de9ff4bb7d9b27fbc5eae85064`".

(e) Compare os resumos obtidos. Mais especificamente, alinhe os resumos obtidos em cada uma das mensagens e, comparando cada caracter do resumo, determine o número de caracteres que são idênticos.

Resposta:

Comparando os resumos MD5 entre as duas frases, conferimos que somente o 17º dos 32 caracteres gerados pelo resumo é igual. Já comparando os resumos SHA1 entre as duas frases, conferimos que apenas as posições 17 e 23 dos 40 caracteres gerados pelo resumo são iguais. Ou seja, ao modificar um único byte da mensagem M, os resumos gerados são muito diferentes.

(f) Obtenha uma mensagem que tenha um resumo parecido com a mensagem do item (c) quando utilizamos MD5. Ou seja, determine M' tal que seu resumo tenha um número maior de bytes iguais ao resumo desta mensagem.

Qual é sua mensagem e quantos bytes são iguais?

Resposta:

O aluno deve procurar por uma mensagem M qualquer que tenha mais de dois caracteres iguais. Por exemplo, a mensagem "Estamos testando funções de hash!", cujo hash MD5 é "`54117121ad214cbdd64e823f71a3ca72`" e possui 2 caracteres iguais.

[1] Dica: no Linux utilize os programas *md5sum* e *sha1sum* para obter os respectivos resumos; cuidado para não inserir o caracter terminador `\n`.