Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AD2 – 2º semestre de 2014 – GABARITO

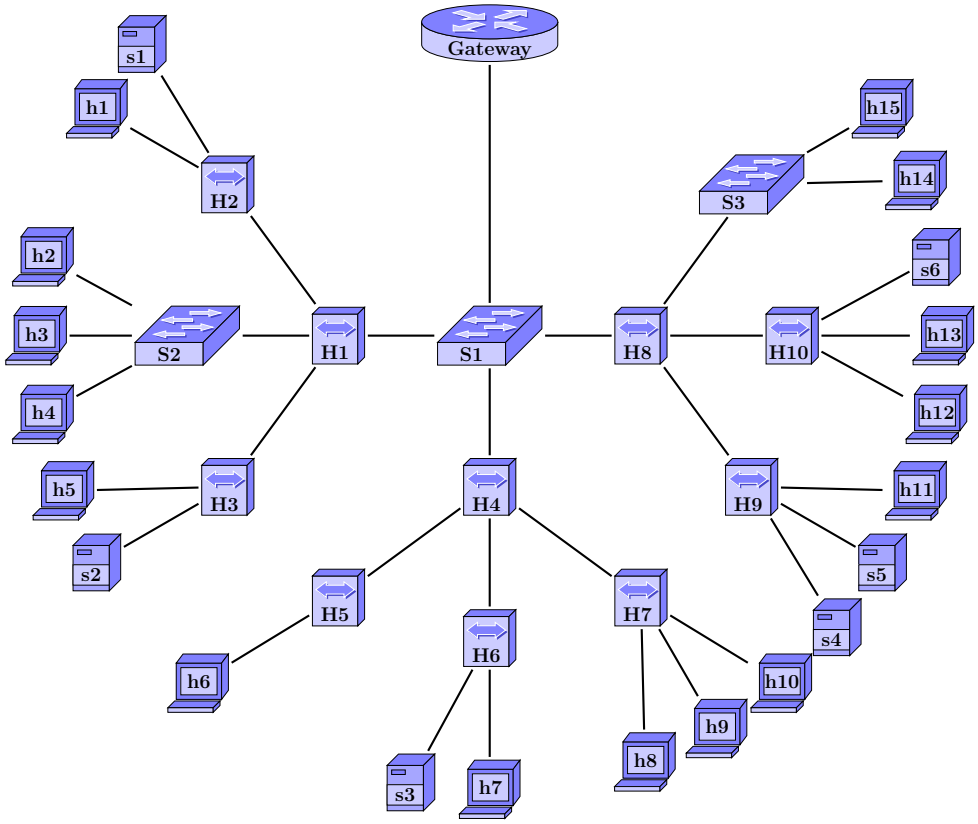
IMPORTANTE: O objetivo desta avaliação é consolidar seus conhecimentos em temas que são fundamentais para o entendimento desta disciplina. A avaliação é formada por diversos exercícios objetivos que irão contribuir para o melhor entendimento de conceitos fundamentais. O entendimento destes conceitos será medido nas APs. Desta forma, é importante você realizar e compreender todos os exercícios desta avaliação, mesmo aqueles que possuem pontuação zerada.

Esta avaliação possui 11 questões e soma 100 pontos, correspondentes à nota máxima (10).

Questão 1 ..... 10 pontos

Apesar de ambos serem equipamentos que atuam na camada de enlace, uma das principais diferenças entre *hubs* e *switches* está na ocorrência de colisões. Neste exercício, iremos compreender melhor o que isto significa.

Considere a seguinte rede local, composta por equipamentos de quatro tipos: estações (h), servidores (s), hubs (H) e switches (S). A única saída desta rede local para a Internet é através do gateway apresentado na ilustração.



(a) Para cada par de estações a seguir, determine se irá ocorrer uma colisão caso elas transmitam dados para a Internet simultaneamente, ou se as transmissões terão sucesso.

i. h9 **não colide** com h11
ii. h6 **colide** com h10
iii. h2 **não colide** com h6
iv. h6 **não colide** com h2
v. h1 **não colide** com h13
vi. h7 **colide** com h9
vii. h13 **colide** com h15
viii. h1 **colide** com h3
ix. h1 **não colide** com h8

(b) Um domínio de colisão é definido como sendo um segmento de rede (conjunto de enlaces) em que sempre ocorrerá colisão se houver duas transmissões simultâneas, mas que não causa colisão com nenhuma transmissão que ocorra fora do segmento. Equipamentos com apenas um enlace (como estações e servidores) fazem parte de apenas um domínio de colisão, enquanto equipamentos com mais de um enlace (como hubs e switches) podem fazer parte de mais de um domínio de colisão.

Identifique os domínios de colisão desta rede.

Resposta:

Domínio 1: h1 / h5 / H1 / H2 / H3 / s1 / s2 / S1 / S2
Domínio 2: h6 / h7 / h8 / h9 / h10 / H4 / H5 / H6 / H7 / s3 / S1
Domínio 3: h11 / h12 / h13 / H8 / H9 / H10 / s4 / s5 / s6 / S1 / S3
Domínio 4: h2 / S2
Domínio 5: h3 / S2
Domínio 6: h4 / S2
Domínio 7: h14 / S3
Domínio 8: h15 / S3

Questão 2 ..... 10 pontos

A ocorrência de colisões também afeta a vazão da rede, isto é, a taxa com que a rede consegue transmitir dados, e neste exercício iremos explorar a relação entre estas duas características.

Considere a mesma rede local da questão anterior. Suponha que todos os enlaces da rede, exceto o enlace entre o switch S1 e o gateway, possuem a capacidade de 100 Mbps.

(a) Em cada item a seguir, são apresentadas transmissões simultâneas de servidores para estações. Considere que, em caso de meio compartilhado entre transmissões, a banda disponível é dividida igualmente entre elas. Determine a vazão de cada transmissão (note que duas transmissões simultâneas podem apresentar vazões diferentes).

i. s1 → h5 — **50 Mbps** , s2 → h1 — **50 Mbps** , s3 → h14 — **100 Mbps**
ii. s5 → h2 — **33 Mbps** , s4 → h10 — **33 Mbps** , s6 → h9 — **33 Mbps**
iii. s1 → h4 — **33 Mbps** , s2 → h14 — **33 Mbps** , s1 → h14 — **33 Mbps**
iv. s3 → h1 — **50 Mbps** , s1 → h9 — **50 Mbps** , s6 → h14 — **100 Mbps**

(b) Considere um cenário em que todas as estações e todos o servidores desejam trocar dados com a Internet simultaneamente. Suponha que a taxa máxima de cada uma destas comunicações seja de 20 Mbps. A capacidade máxima dos enlaces permanecem iguais a 100 Mbps.

Determine qual deve ser a capacidade mínima do enlace entre o switch S1 e o gateway para que ele não seja o gargalo desta rede.

Resposta:

A capacidade mínima desse enlace deve ser igual a vazão máxima entre a Internet e o conjunto de servidores e estações desta rede. Essa vazão é igual a 120 Mbps.

Questão 3 ..... 10 pontos

O objetivo desta questão é compreender como funcionam dois algoritmos de funcionamento dos *switches*: o algoritmo de encaminhamento de pacotes e o algoritmo de aprendizado.

Considere a seguinte rede local, onde cada enlace é identificado por um número. Abaixo também são apresentadas as tabelas de encaminhamento de cada switch nesta rede.

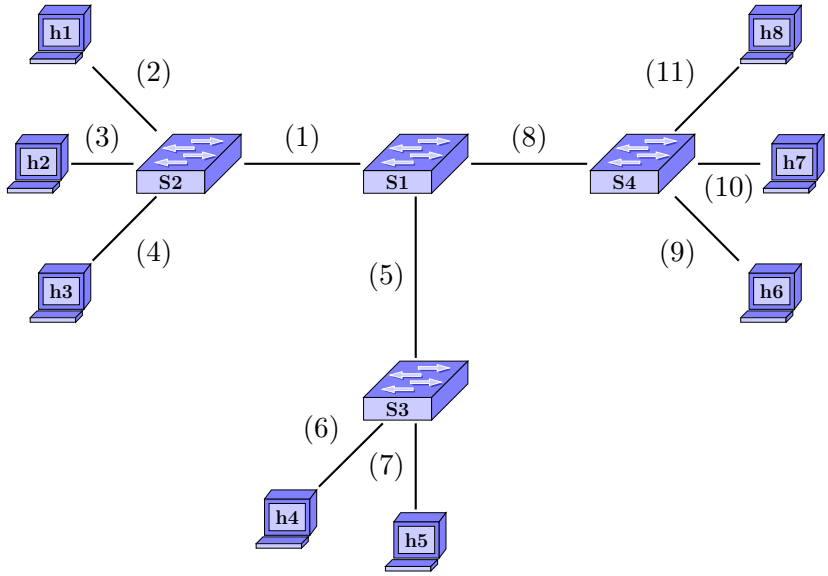


Tabela de S1	
Destino	Interface
h2	1
h7	8
h5	5
h6	8
h8	8

Tabela de S2	
Destino	Interface
h2	3
h7	1
h5	1
h8	1

Tabela de S3	
Destino	Interface
h2	5
h5	7
h6	5
h8	5

Tabela de S4	
Destino	Interface
h2	8
h7	10
h5	8
h6	9
h8	11

Em cada um dos itens a seguir, apresentamos as estações origem e destino de um quadro enviado nesta rede. Para cada um destes quadros, determine:

(a) por quais enlaces o quadro será transmitido;

(b) quais entradas serão criadas na tabela de encaminhamento dos switches.

Considere que os quadros são enviados em sequência e, portanto, toda entrada criada em alguma tabela de encaminhamento na transmissão de um quadro será utilizada pelos switches na transmissão dos quadros seguintes.

i. h2 → h6

Transmitido pelos enlaces: 1, 2, 3, 4, 8, 9
Nenhuma entrada é criada.

ii. h4 → h1

Transmitido pelos enlaces: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Entradas criadas:

- **Tabela do switch S1:** | **Destino: h4** | **Interface: 5** |
- **Tabela do switch S2:** | **Destino: h4** | **Interface: 1** |
- **Tabela do switch S3:** | **Destino: h4** | **Interface: 6** |
- **Tabela do switch S4:** | **Destino: h4** | **Interface: 8** |

iii. h8 → h2

Transmitido pelos enlaces: 1, 3, 8, 11
Nenhuma entrada é criada.

iv. h1 → h5

Transmitido pelos enlaces: 1, 2, 5, 7
Entradas criadas:

- **Tabela do switch S1:** | **Destino: h1** | **Interface: 1** |
- **Tabela do switch S2:** | **Destino: h1** | **Interface: 2** |
- **Tabela do switch S3:** | **Destino: h1** | **Interface: 5** |

v. h3 → h1

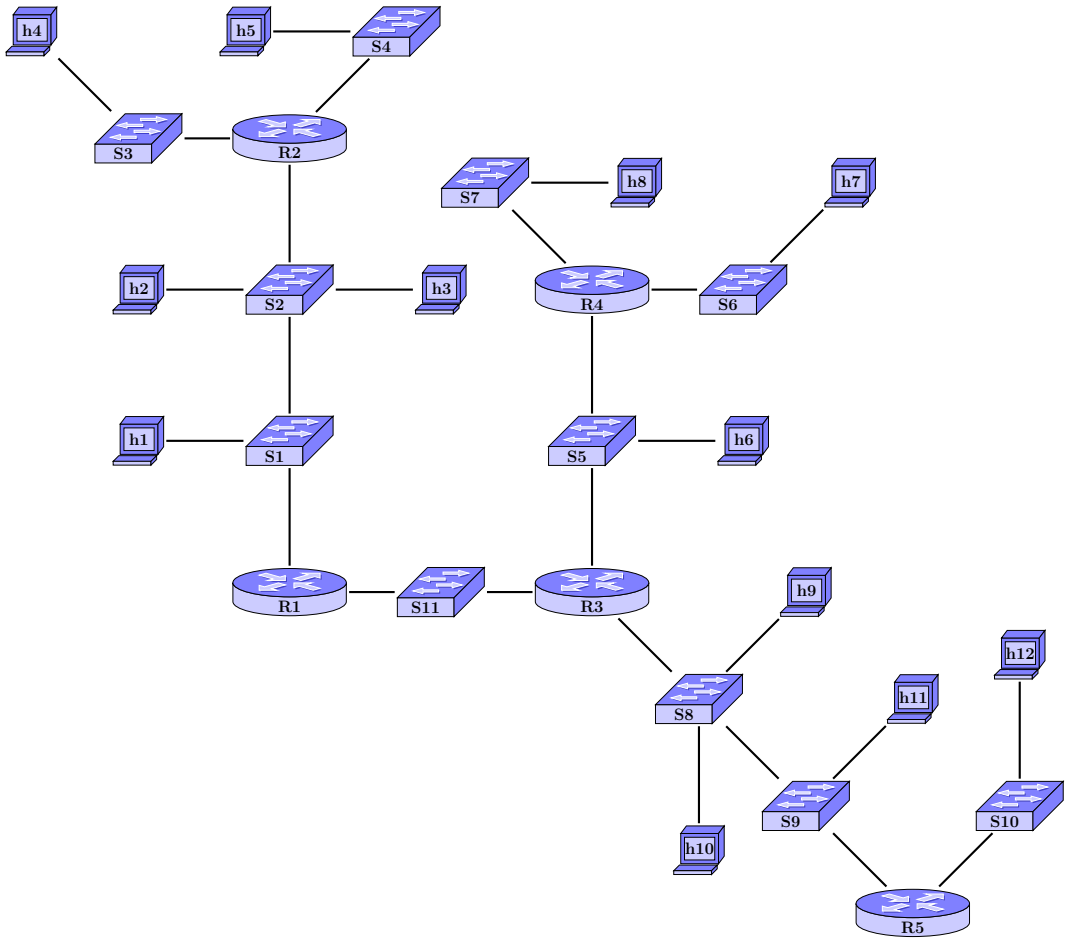
Transmitido pelos enlaces: 2, 4
Entradas criadas:

- **Tabela do switch S2:** | **Destino: h3** | **Interface: 4** |

Questão 4 ..... 10 pontos

O objetivo deste exercício é compreender melhor o que significam as camadas de rede e de enlace na Internet.

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



Em cada um dos itens abaixo, são apresentadas duas estações entre as quais existe um fluxo de dados UDP na camada de rede. Os datagramas deste fluxo devem ser encapsulados em quadros na camada de enlace para que a transmissão seja realizada. Para cada um destes fluxos:

(a) determine o caminho que os datagramas irão percorrer na camada de rede;

(b) determine quantos quadros diferentes serão utilizados para encapsular cada datagrama em seu percurso;

(c) determine o caminho que estes quadros irão percorrer na camada de enlace;

i. h12 → h2

Caminho na camada de rede: h12 → R5 → R3 → R1 → h2;
Encapsulado em 4 quadros;
Caminho (total) na camada de enlace: h12 → S10 → R5 → S9 → S8 → R3 → S11 → R1 → S1 → S2 → h2.

ii. h12 → h7

Caminho na camada de rede: h12 → R5 → R3 → R4 → h7;
Encapsulado em 4 quadros;
Caminho (total) na camada de enlace: h12 → S10 → R5 → S9 → S8 → R3 → S5 → R4 → S6 → h7.

iii. h8 → h10

Caminho na camada de rede: h8 → R4 → R3 → h10;

Encapsulado em 3 quadros;
Caminho (total) na camada de enlace: h8 → S7 → R4 → S5 → R3 → S8 → h10.

iv. h2 → h1

Caminho na camada de rede: h2 → h1;
Encapsulado em 1 quadros;
Caminho (total) na camada de enlace: h2 → S2 → S1 → h1.

v. h7 → h3

Caminho na camada de rede: h7 → R4 → R3 → R1 → h3;
Encapsulado em 4 quadros;
Caminho (total) na camada de enlace: h7 → S6 → R4 → S5 → R3 → S11 → R1 → S1 → S2 → h3.

Questão 5 ..... 10 pontos

O objetivo desta questão é compreender como funciona o protocolo ARP, protocolo da camada de enlace utilizado para resolver endereços entre as camadas de rede e enlace.

Considere a mesma rede e o mesmo conjunto de fluxos da questão anterior (listados novamente abaixo), e suponha que as tabelas ARP de todos os equipamentos da rede estão vazias no início de cada um destes fluxos. Uma estação origem, para encapsular o primeiro datagrama do fluxo em um quadro, deve enviar uma *ARP query* em broadcast contendo um endereço IP, a fim de determinar quem será o destino deste quadro.

Para cada uma das estações origem, determine:[1]

(a) o equipamento cujo endereço IP estará contido na *ARP query*;

(b) quais equipamentos irão receber a *ARP query*;

(c) qual equipamento irá responder a *ARP query*.

i. h12 → h2

ARP query contém IP de R5; é recebido por R5, S10 e h12, e é respondido por R5.

ii. h12 → h7

ARP query contém IP de R5; é recebido por R5, S10 e h12, e é respondido por R5.

iii. h8 → h10

ARP query contém IP de R4; é recebido por R4, S6, S7, h7 e h8, e é respondido por R4.

iv. h2 → h1

ARP query contém IP de h1; é recebido por R1, R2, S1, S2, h1, h2 e h3, e é respondido por h1.

v. h7 → h3

ARP query contém IP de R4; é recebido por R4, S6, S7, h7 e h8, e é respondido por R4.

[1] Dica: utilize os caminhos identificados na questão anterior.

Questão 6 ..... 10 pontos

O objetivo deste exercício é compreender melhor a ocorrência de colisões entre estações compartilhando acesso sem fio ao meio.

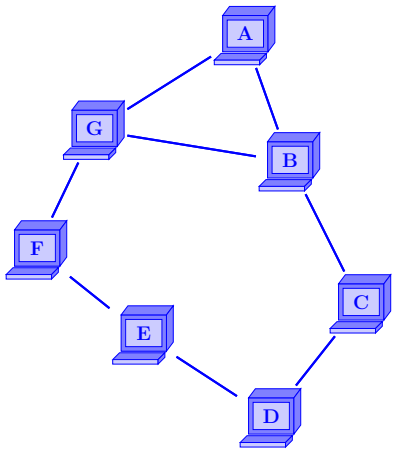
Considere uma rede sem fio não estruturada (*ad hoc*), na qual diversas estações tentam transmitir dados umas para as outras. As distâncias entre elas são dadas na tabela abaixo:

	A	B	C	D	E	F	G
A		3.5 m	7.7 m	10.1 m	8.4 m	7.9 m	4.7 m
B	3.5 m		4.2 m	6.8 m	6.0 m	7.1 m	5.2 m
C	7.7 m	4.2 m		3.8 m	5.8 m	8.7 m	8.4 m
D	10.1 m	6.8 m	3.8 m		4.0 m	7.6 m	8.9 m
E	8.4 m	6.0 m	5.8 m	4.0 m		3.6 m	5.6 m
F	7.9 m	7.1 m	8.7 m	7.6 m	3.6 m		3.5 m
G	4.7 m	5.2 m	8.4 m	8.9 m	5.6 m	3.5 m	

Suponha que uma estação consegue ouvir a transmissão de outra se elas se encontram a uma distância de 5.2 m ou menos. Caso contrário, devido ao desvanecimento do sinal, uma estação estará oculta para a outra.

(a) Construa o grafo de conectividade desta rede. Neste grafo, vértices são estações, e uma aresta entre duas estações indica que elas ouvem a transmissão uma da outra.

Resposta:



(b) Suponha que duas transmissões ocorrem simultaneamente. Diremos que ocorre colisão sempre que alguma estação desta rede escutar ambas as transmissões.

Para cada par de transmissões a seguir, determine se irá ocorrer uma colisão ou não.

i. A → B / E → D — **Não há colisão**

ii. E → F / A → G — **Não há colisão**

iii. D → C / E → F — **Há colisão**

iv. E → D / F → G — **Há colisão**

v. C → B / D → E — **Há colisão**

vi. B → C / D → E — **Há colisão**

Questão 7 ..... 10 pontos

Uma das técnicas de acesso a meio compartilhado mais utilizadas em redes sem fio é a técnica CDMA. Nesta técnica, códigos ortogonais são utilizados pelas estações para transmitir seus dados, de forma que o receptor possa dissociar as transmissões. O objetivo desta questão é entender o funcionamento desta técnica e a importância de escolher códigos ortogonais.

Considere uma rede sem fio estruturada, em que estações enviam dados simultaneamente para um ponto de acesso. A tabela a seguir apresenta os códigos utilizados pelas estações e os bits que elas desejam transmitir. Note que os códigos são ortogonais uns aos outros.

Estação	Código	Bits a transmitir
Estação 1	(1 , -1 , -1 , 1)	0 0 1 1
Estação 2	(1 , 1 , -1 , -1)	1 0 1 0
Estação 3	(-1 , 1 , -1 , 1)	0 0 0 1

(a) Determine a sequência codificada que cada estação irá enviar para o ponto de acesso.

Resposta:

Estação 1 envia:
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (1 , -1 , -1 , 1)
- (1 , -1 , -1 , 1)

Estação 2 envia:
- (1 , 1 , -1 , -1)
- (0 , 0 , 0 , 0)
- (1 , 1 , -1 , -1)
- (0 , 0 , 0 , 0)

Estação 3 envia:
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (-1 , 1 , -1 , 1)

(b) Suponha que todas as estações comecem a transmitir suas sequências simultaneamente. Determine a sequência de dados que será recebida pelo ponto de acesso.

Resposta:

As sequências transmitidas serão somadas bit a bit no meio, logo o ponto de acesso irá receber a sequência (1 , 1 , -1 , -1 , 0 , 0 , 0 , 0 , 2 , 0 , -2 , 0 , 0 , 0 , -2 , 2).

(c) Apresente os cálculos realizados pelo ponto de acesso para obter os bits transmitidos por cada estação. O ponto de acesso recebe estes bits com sucesso?

Resposta:

Todas as decodificações ocorreram com sucesso. Para a estação 1:
- (1 , 1 , -1 , -1) · (1 , -1 , -1 , 1)/4 = 0/4 = 0
- (0 , 0 , 0 , 0) · (1 , -1 , -1 , 1)/4 = 0/4 = 0
- (2 , 0 , -2 , 0) · (1 , -1 , -1 , 1)/4 = 4/4 = 1
- (0 , 0 , -2 , 2) · (1 , -1 , -1 , 1)/4 = 4/4 = 1

Para a estação 2:
- (1 , 1 , -1 , -1) · (1 , 1 , -1 , -1)/4 = 4/4 = 1
- (0 , 0 , 0 , 0) · (1 , 1 , -1 , -1)/4 = 0/4 = 0
- (2 , 0 , -2 , 0) · (1 , 1 , -1 , -1)/4 = 4/4 = 1
- (0 , 0 , -2 , 2) · (1 , 1 , -1 , -1)/4 = 0/4 = 0

Para a estação 3:
- (1 , 1 , -1 , -1) · (-1 , 1 , -1 , 1)/4 = 0/4 = 0
- (0 , 0 , 0 , 0) · (-1 , 1 , -1 , 1)/4 = 0/4 = 0
- (2 , 0 , -2 , 0) · (-1 , 1 , -1 , 1)/4 = 0/4 = 0
- (0 , 0 , -2 , 2) · (-1 , 1 , -1 , 1)/4 = 4/4 = 1

(d) Considere agora um novo cenário, em que estas mesmas estações transmitem os mesmos bits, mas utilizando os seguintes códigos:

Estação	Código
Estação 1	(1 , 1 , 1 , -1)
Estação 2	(-1 , -1 , -1 , -1)
Estação 3	(1 , -1 , -1 , -1)

Note que, desta vez, os códigos não são ortogonais dois a dois. Repita os itens anteriores e determine se as transmissões ocorrem com sucesso.

Resposta:

Estação 1 envia:
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (1 , 1 , 1 , -1)
- (1 , 1 , 1 , -1)

Estação 2 envia:
- (-1 , -1 , -1 , -1)
- (0 , 0 , 0 , 0)
- (-1 , -1 , -1 , -1)
- (0 , 0 , 0 , 0)

Estação 3 envia:
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (0 , 0 , 0 , 0)
- (1 , -1 , -1 , -1)

Novamente as sequências transmitidas serão somadas no meio e o ponto de acesso irá receber a sequência (-1 , -1 , -1 , -1 , 0 , 0 , 0 , 0 , 0 , 0 , 0 , -2 , 2 , 0 , 0 , -2) para decodificação.

Decodificação dos bits da estação 1:
- (-1 , -1 , -1 , -1) · (1 , 1 , 1 , -1)/4 = -2/4 = -0.5 = ?
- (0 , 0 , 0 , 0) · (1 , 1 , 1 , -1)/4 = 0/4 = 0
- (0 , 0 , 0 , -2) · (1 , 1 , 1 , -1)/4 = 2/4 = 0.5 = ?
- (2 , 0 , 0 , -2) · (1 , 1 , 1 , -1)/4 = 4/4 = 1

Decodificação dos bits da estação 2:
- (-1 , -1 , -1 , -1) · (-1 , -1 , -1 , -1)/4 = 4/4 = 1
- (0 , 0 , 0 , 0) · (-1 , -1 , -1 , -1)/4 = 0/4 = 0
- (0 , 0 , 0 , -2) · (-1 , -1 , -1 , -1)/4 = 2/4 = 0.5 = ?
- (2 , 0 , 0 , -2) · (-1 , -1 , -1 , -1)/4 = 0/4 = 0

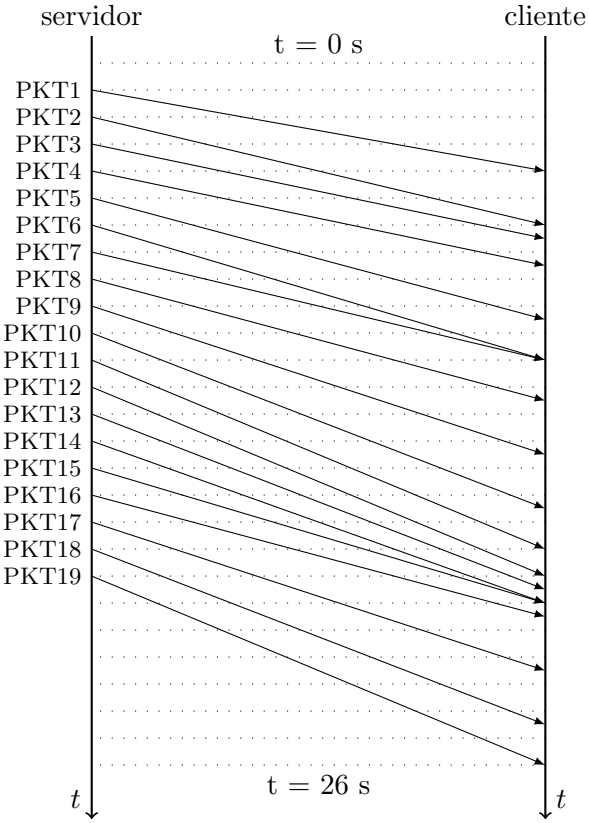
Decodificação dos bits da estação 3:
- (-1 , -1 , -1 , -1) · (1 , -1 , -1 , -1)/4 = 2/4 = 0.5 = ?
- (0 , 0 , 0 , 0) · (1 , -1 , -1 , -1)/4 = 0/4 = 0
- (0 , 0 , 0 , -2) · (1 , -1 , -1 , -1)/4 = 2/4 = 0.5 = ?
- (2 , 0 , 0 , -2) · (1 , -1 , -1 , -1)/4 = 4/4 = 1

Desta vez, os bits enviados pelas estações não são recuperados pelo ponto de acesso, logo a transmissão não ocorreu com sucesso.

Questão 8 ..... 10 pontos

Para compensar pelo *jitter* observado na Internet como consequência do seu modelo "*best effort*" de serviço, aplicações de transmissão de vídeo por *streaming* utilizam técnicas de bufferização no cliente. Nestas técnicas, o cliente irá armazenar os dados da mídia a ser reproduzida em um *buffer* antes da reprodução, com o objetivo de atrasá-la e, com isso, melhor a qualidade da reprodução. O objetivo desta questão é compreender o funcionamento destes mecanismos de bufferização de cliente.

Considere o seguinte cenário, em que um servidor transmite pacotes por *streaming* uma sequência de pacotes de um vídeo para um cliente. O diagrama a seguir ilustra esta transmissão. Note que o pacote PKT1 foi transmitido no instante de tempo t = 1 s, o pacote PKT2, no instante t = 2 s, e assim por diante.



(a) Determine o instante de recepção de cada pacote e calcule seu atraso de propagação.

Resposta:

PKT1 Transmissão em t = 1.0 s, recepção em t = 4.0 s: atraso de 3.0 s
PKT2 Transmissão em t = 2.0 s, recepção em t = 6.0 s: atraso de 4.0 s
PKT3 Transmissão em t = 3.0 s, recepção em t = 6.5 s: atraso de 3.5 s
PKT4 Transmissão em t = 4.0 s, recepção em t = 7.5 s: atraso de 3.5 s
PKT5 Transmissão em t = 5.0 s, recepção em t = 9.5 s: atraso de 4.5 s
PKT6 Transmissão em t = 6.0 s, recepção em t = 11.0 s: atraso de 5.0 s
PKT7 Transmissão em t = 7.0 s, recepção em t = 11.0 s: atraso de 4.0 s
PKT8 Transmissão em t = 8.0 s, recepção em t = 12.5 s: atraso de 4.5 s
PKT9 Transmissão em t = 9.0 s, recepção em t = 14.5 s: atraso de 5.5 s
PKT10 Transmissão em t = 10.0 s, recepção em t = 16.5 s: atraso de 6.5 s
PKT11 Transmissão em t = 11.0 s, recepção em t = 18.0 s: atraso de 7.0 s
PKT12 Transmissão em t = 12.0 s, recepção em t = 19.0 s: atraso de 7.0 s
PKT13 Transmissão em t = 13.0 s, recepção em t = 19.5 s: atraso de 6.5 s
PKT14 Transmissão em t = 14.0 s, recepção em t = 20.0 s: atraso de 6.0 s
PKT15 Transmissão em t = 15.0 s, recepção em t = 20.0 s: atraso de 5.0 s
PKT16 Transmissão em t = 16.0 s, recepção em t = 20.5 s: atraso de 4.5 s
PKT17 Transmissão em t = 17.0 s, recepção em t = 22.5 s: atraso de 5.5 s
PKT18 Transmissão em t = 18.0 s, recepção em t = 24.5 s: atraso de 6.5 s
PKT19 Transmissão em t = 19.0 s, recepção em t = 26.0 s: atraso de 7.0 s

(b) Considere o seguinte mecanismo de bufferização no cliente: o cliente possui um buffer de capacidade infinita, no qual armazena todos os pacotes assim que chegam, e o vídeo começará a ser reproduzido somente após um atraso pré-determinado (a ser escolhido), que conta a partir da chegada do primeiro pacote. Qualquer pacote que chegue após o

instante em que deveria ser reproduzido é considerado perdido.

Suponha que você pode escolher entre as opções de atraso de reprodução a seguir. Qual será a porcentagem de pacotes perdidos nesta transmissão, para cada opção?

i. 0.5 s **: 84.2%** ii. 2.5 s **: 36.8%** iii. 3.0 s **: 31.6%**

(c) Para este mecanismo, qual deve ser o atraso de reprodução mínimo para que nenhum pacote desta transmissão seja perdido?

Resposta:

Todos os pacotes serão reproduzidos se o atraso for de 4.0 s ou maior.

(d) Considere agora este segundo mecanismo de bufferização: novamente o cliente possui um buffer infinito, mas agora ele começará a reproduzir o vídeo após um certo número de pacotes (a ser definido) ter chegado. Pacotes que chegarem após o instante em que deveriam ser reproduzidos são considerados perdidos.

Em cada item a seguir, será apresentada uma opção de atraso de reprodução. Qual será a porcentagem de pacotes perdidos para cada opção, para a transmissão apresentada?

i. 2 pacotes **: 47.4%** ii. 3 pacotes **: 36.8%** iii. 4 pacotes **: 15.8%**

(e) Para este segundo mecanismo, quantos pacotes, no mínimo, o cliente deve esperar chegar para começar a reprodução, se não quiser perdas nesta transmissão?

Resposta:

Basta aguardar a chegada de 5 pacotes, para que todos sejam reproduzidos.

Questão 9 ..... 10 pontos

O objetivo desta questão é compreender como funciona o mecanismo de *forward error correction*, ou FEC, e como ele auxilia a recuperação de pacotes de vídeo sem retransmissão.

Considere um servidor realizando *streaming* de vídeo para um cliente. Serão transmitidos 21 pacotes, numerados de 1 a 21, em slots de tempo pré-determinados (um pacote por slot).

Além disso, o servidor irá implementar o seguinte esquema de redundância FEC: para cada k pacotes, o servidor irá criar um pacote adicional FEC contendo o XOR destes pacotes e o transmitirá ao cliente. Caso o último grupo tenha menos que k pacotes, o último FEC será aplicado nos pacotes restantes.

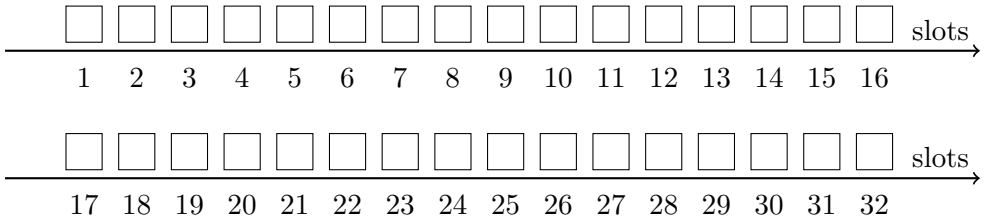
Suponha que o servidor pode optar por implementar um esquema FEC com k = 2, 3 ou 6. *Para cada um destes esquemas*, responda as seguintes perguntas:

(a) No total, quantos pacotes (de vídeo ou FEC) ele irá transmitir para o cliente?

Resposta:

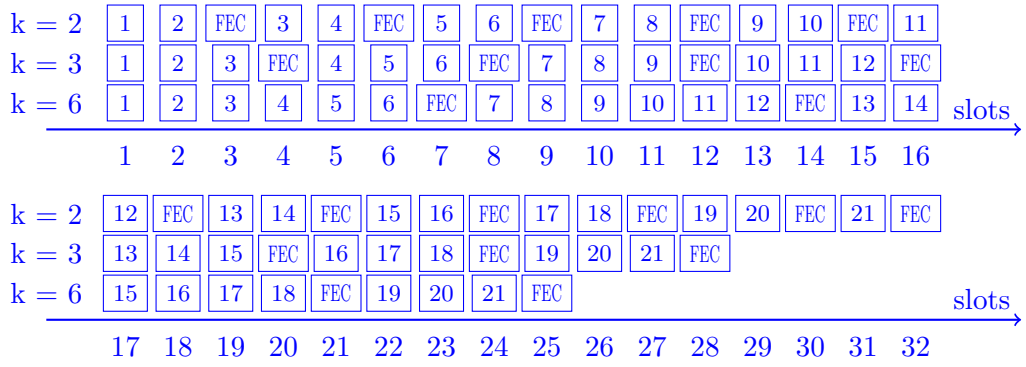
Para k = 2, serão transmitidos 32 pacotes.
Para k = 3, serão transmitidos 28 pacotes.
Para k = 6, serão transmitidos 25 pacotes.

(b) Considere o diagrama a seguir:

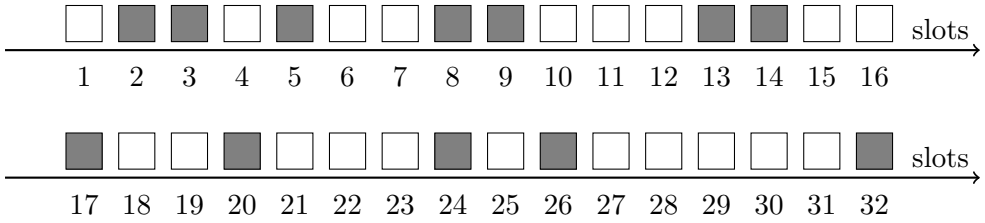


Cada quadrado neste diagrama representa um slot de transmissão. Preencha esse diagrama indicando, em cada slot, se foi transmitido um pacote de vídeo, um pacote FEC, ou se não houve transmissão. Para os pacotes de vídeo, indique também o número do pacote transmitido.

Resposta:

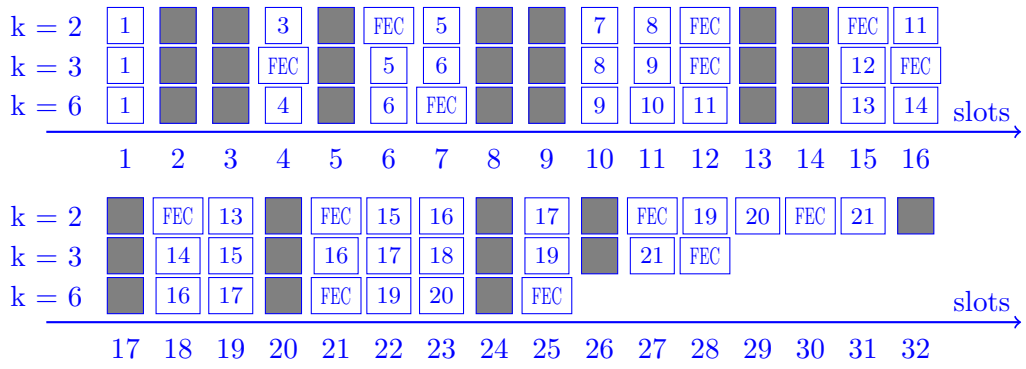


(c) Suponha agora que seja observado o padrão de perdas ilustrado a seguir:



Nesta ilustração, quadrados brancos indicam transmissões com sucesso e quadrados cinzas indicam pacotes perdidos. Preencha novamente o diagrama anterior, agora pelo ponto de vista do cliente; isto é, indique se foi recebido um pacote de vídeo (e qual o seu número), um pacote FEC, se o pacote enviado foi perdido ou se não houve transmissão.

Resposta:



(d) Utilizando o diagrama construído no item anterior, determine quais pacotes de vídeo o cliente não irá receber. Determine também quais destes pacotes o cliente será capaz de recuperar com o uso do pacote FEC.

Resposta:

k = 2 Os pacotes 2, 4, 6, 9, 10, 12, 14 e 18 serão perdidos na transmissão. Destes, o cliente poderá, com o uso dos pacotes FEC, recuperar os pacotes 4, 12, 14 e 18.

k = 3 Os pacotes 2, 3, 4, 7, 10, 11, 13 e 20 serão perdidos na transmissão. Destes, o cliente poderá, com o uso dos pacotes FEC, recuperar os pacotes 7 e 20.

k = 6 Os pacotes 2, 3, 5, 7, 8, 12, 15, 18 e 21 serão perdidos na transmissão. O esquema FEC somente irá ajudar a recuperar o pacote 21.

(e) Qual a porcentagem de pacotes reproduzidos com sucesso pelo cliente?

Resposta:

A fração de pacotes reproduzidos será igual a 81.0% (com k = 2), 71.4% (com k = 3) ou 61.9% (com k = 6).

Questão 10 ..... 5 pontos

O objetivo desta questão é compreender o funcionamento de sistemas de criptografia baseados em chaves público-privada. Nestes sistemas, as entidades comunicantes deverão, cada uma, gerar pares de chaves complementares, uma das quais ficará de posse exclusiva da entidade em questão (chave privada), com a outra sendo disponibilizada a outros (chave pública).

(a) Em termos operacionais, qual é a principal vantagem da criptografia baseada em chaves público-privada?

Resposta:

Permitir a comunicação confidencial entre duas partes sem que estas compartilhem qualquer segredo. Ou seja, garantir a confidencialidade na comunicação sem demandar uma chave compartilhada.

(b) Em termos operacionais, qual é a principal desvantagem da criptografia baseada em chaves público-privada?

Resposta:

Informar a chave pública a outra parte. Para que o sistema funcione adequadamente, as duas partes precisam conhecer suas respectivas chaves públicas. Esta informação precisa ser comunicada de alguma forma, o que pode comprometer a criptografia se não for realizada corretamente (vide ataque do homem-no-meio).

(c) Como podemos superar a principal desvantagem operacional da criptografia baseada em chaves público-privada?

Resposta:

A troca de chaves pública entre as partes comunicantes, que é a principal desvantagem operacional da criptografia baseada em chaves público-privada, pode ser superada utilizando autoridades de certificação e certificados. Em particular, o problem é resolvido quando as duas partes comunicantes possuem certificados de sua chave pública assinados por uma autoridade de certificação conhecida (i.e., conheçam a chave pública da autoridade de certificação). Desta forma, uma parte pode transmitir seu certificado (que possui sua chave pública) e a outra parte pode verificar sua autenticidade (e consequentemente, que a chave pública está correta), pois o mesmo está assinado por uma autoridade de certificação conhecida. Este é o procedimento adotado pelo HTTPS, por exemplo, que utiliza chave público-privada e gera uma mensagem de alerta quando o browser recebe um certificado assinado por uma autoridade de certificação desconhecida.

Questão 11 ..... 5 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: "Estamos testando funções de hash!"[2] Apresente o resumo em formato hexadecimal.

Resposta:

O resumo MD5 desta frase é "`54117121ad214cbdd64e823f71a3ca72`", e o seu resumo SHA1 é "`258c7903aa192777e47b83b16121efaa8fa50e77`".

(d) Repita o item anterior para a seguinte mensagem (sem aspas): "Estamos testando funções de hash." 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 "`9465e7df97be6dea5a1ad38eb2d6afe1`", e utilizando o SHA1 é "`85742fda123137c4eafe4b1c2cab9dbb57b927f7`".

(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 2º dos 32 caracteres gerados pelo resumo é igual. Já comparando os resumos SHA1 entre as duas frases, conferimos que apenas as posições 2, 14, 17 e 40 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 "Existem diversos algoritmos de hash.", cujo hash MD5 é "`d36cb2a6724707d5dad7652800ab3bc7`" e possui 2 caracteres iguais.

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