



Departamento de Informática  
Faculdade de Ciências e Tecnologia  
UNIVERSIDADE NOVA DE LISBOA

**Licenciatura em Engenharia Informática — Exame de Redes de Computadores  
Ano lectivo: 2011/2012 –Época de Recurso — (20 de Julho de 2012)**

- **O Exame é composto por 10 questões e respectivas alíneas e está impresso em 9 páginas**
- **Pode-se responder a lápis mas não se podem separar as folhas umas das outras**
- **A interpretação do enunciado é uma componente da avaliação**
- **Não se podem usar calculadores nem telemóveis durante a resolução, sendo distribuídas folhas de rascunho**
- **Em caso de desistência deve entregar-se o exame com a menção “DESISTI”. Versão A**

Aluno nº \_\_\_\_\_ Nome: \_\_\_\_\_

**Questão 1**

Um servidor WEB pretende contar o nº de vezes que é visitado por um dado utilizador U (número de vezes que recebe uma mensagem HTTP GET na sequência de um pedido do utilizador U).

- a) Sabendo que U usa sempre o mesmo computador portátil, em diferentes localizações, como pode essa contabilização ser feita ?

**No servidor WEB poderia usar como mecanismo para essa contabilização o seguinte:**

- b) Sabendo que U não usa sempre o mesmo computador.

**No servidor WEB poderia usar como mecanismo para essa contabilização o seguinte:**

## Questão 2

Dois *routers* **R1** e **R2** estão ligados por um canal de dados com a velocidade de transmissão de **1 Mbps** e com um tempo de propagação de **10 ms**. O computador **A** está ligado directamente ao *router* **R1** através de um canal com tempo de propagação desprezável e velocidade de transmissão de **1 Gbps**. O computador **B** está ligado a **R2** por um canal com as mesmas características do que liga **A** a **R1**. Em diversas ocasiões fizeram-se testes executando **ping de A para B** com pacotes com **10.000 bits**.

a) No primeiro teste obtiveram-se os resultados abaixo. Acha os mesmos possíveis ou houve algum engano durante o teste? Escolha uma das opções e risque a outra. Em qualquer caso justifique a sua resposta.

```
--- .... ping statistics ---  
10 packets transmitted, 10 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 4.04 / 5.19 / 6.81 / 0.4 ms
```

**Os resultados apresentados são possíveis:**  
**Os resultados apresentados NÃO são possíveis:**  
**Justificação:**

b) Em dois testes posteriores, em ocasiões distintas, obtiveram-se os resultados abaixo. O que explica a diferença nos dois casos? Dê a explicação em termos do tratamento pelos *routers* dos pacotes enviados pelo programa **ping**.

```
--- B ping statistics ---  
10 packets transmitted, 10 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 21.04 / 22.19 / 23.81 / 0.4 ms
```

```
--- B ping statistics ---  
10 packets transmitted, 8 packets received, 20% packet loss  
round-trip min/avg/max/stddev = 21.04 / 200.19 / 1030.81 / 450 ms
```

**O que explica a diferença é:**

c) Na situação correspondente à segunda medida (com round-trip min/avg/max/stddev = 21.04 / 200.19 / 1030.81 / 450 ms) era possível ter uma vídeo conferência interactiva entre utilizadores dos computadores A e B ? Escolha uma das opções e risque a outra. Em qualquer caso justifique a sua resposta.

**SIM, a vídeo-conferência interactiva era possível:**  
**NÃO, a vídeo-conferência interactiva não era possível:**  
**Justificação:**

### Questão 3

Suponha que o tempo médio para executar uma interação *request / reply* com um dado servidor DNS é desprezável, quando o servidor de DNS está na rede interna da FCT/UNL e é de 100 ms, quando o servidor DNS está fora da rede da FCT/UNL.

Nas questões abaixo assinale com um circulo a opção **que mais se aproxima** da resposta certa.

- a) Qual o tempo necessário para um cliente dentro da rede da FCT/UNL obter o endereço associado ao nome “streaming.cnn.com” admitindo que o DNS não faz  *caching*  e que o nome existe.

desprezável, 20, 50, 75, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

- b) Como sabe, os servidores DNS podem, ou não, ter a resposta a um pedido de um cliente disponível na sua cache. Tendo isso em consideração, responda às seguintes questões:

- b1) qual é o **TEMPO MÍNIMO** que pode ser necessário para um cliente dentro da rede da FCT/UNL resolver o endereço associado ao nome “streaming.cnn.com” ?

desprezável, 20, 50, 75, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

- b2) qual é o **TEMPO MÁXIMO** que pode ser necessário para um cliente dentro da rede da FCT/UNL resolver o endereço associado ao mesmo nome “streaming.cnn.com” ?

desprezável, 20, 50, 75, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

- c) Admite-se que a taxa de sucesso de os servidores DNS internos à FCT terem a resposta a um pedido de um cliente disponível na sua cache é de 30%. Qual é o **TEMPO MÉDIO** que pode ser necessário a um cliente dentro da rede da FCT/UNL para obter o endereço associado ao nome “streaming.cnn.com”. Admita que quando o nome não está na cache, o servidor está na situação da **a)**.

desprezável, 20, 50, 75, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

- d) Admitindo que os servidores DNS internos à FCT têm na sua cache a seguinte entrada:

|              |    |              |
|--------------|----|--------------|
| cnn.com      | NS | dns1.cnn.com |
| cnn.com      | NS | dns2.cnn.com |
| dns1.cnn.com | A  | 88.10.1.24   |
| dns2.cnn.com | A  | 88.10.2.56   |

e mais nenhuma informação útil à query, indique o tempo necessário a um cliente dentro da rede da FCT/UNL para obter o endereço associado ao nome “streaming.cnn.com”.

desprezável, 20, 50, 75, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

### Questão 4

Um browser WEB na FCT/UNL acede a páginas WEB de forma directa quando estas estão no domínio “fct.unl.pt” e com recurso a um  *proxy*  quando estas estão fora do domínio indicado. Fizeram-se medidas e verificou-se que o “ *cache hit ratio* ” era de 50%, e que o tempo de transferência dos objectos WEB de servidores internos à FCT/UNL para o browser era desprezável quando comparado com o tempo que o proxy levava a fazer o download de objectos WEB disponibilizados por servidores fora da rede da FCT/UNL. Tendo-se verificado que o tempo de acesso a objectos WEB fora da FCT/UNL por computadores que estavam a usar o proxy era em média de 500 ms, qual o tempo médio que o proxy levava a obter os objectos dos servidores externos?

desprezável, 1, 2, 3, 4, 5, 6, 7, 8, 9, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000 ms

### Questão 5

Um computador **A** está ligado a um computador **B** através de um canal com a dimensão de 4.000 Km e uma velocidade de propagação de 200.000 Km / s e por hipótese sem erros. Entre os dois computadores são trocados segmentos de dados com 10.000 bits e cujo tempo de transmissão é de 10 ms. Entre os dois computadores está a executar um protocolo de transferência de dados do tipo janela deslizante com as janelas de emissão e recepção ambas da dimensão de um segmento (com 10.000 bits).

Nas seguintes alíneas, **circunde com um círculo** o resultado que considera correcto (ou o mais perto desse).

- a) Qual a taxa de utilização máxima do canal entre A e B que o protocolo descrito acima permite obter quando as janelas do emissor e do receptor são ambas iguais a um segmento de 10.000 bits. O resultado deve ser expresso **em percentagem**.

1 2 3 4 5 12 16 18 20 25 28 30 40 50 55 66 74 80 85 92 100 110

- b) Qual a taxa de utilização máxima do canal entre A e B que o protocolo descrito acima permite obter quando a janela do emissor é igual a um segmento de 10.000 bits e a do receptor a 2 segmentos de 10.000 bits cada. O resultado deve ser expresso **em percentagem**.

1 2 3 4 5 12 16 18 20 25 28 30 40 50 55 66 74 80 85 92 100 110

- c) Qual a taxa de utilização máxima do canal entre A e B que o protocolo descrito acima permite obter quando a janela do emissor é igual a dois segmentos de 10.000 bits cada e a do receptor a 1 segmento de 10.000 bits. O resultado é expresso **em percentagem**.

1 2 3 4 5 12 16 18 20 25 28 30 40 50 55 66 74 80 85 92 100 110

- d) Quanto tempo leva a transmitir do emissor para o receptor um ficheiro com a dimensão de 10 segmentos usando a versão do protocolo indicado na c). A transferência só termina quando o emissor receber o último ACK. O resultado deve ser expresso **em mili segundos (ms)**.

10 20 30 40 50 100 120 160 180 200 250 280 300 400 500 550 660 740  
800 850 920 1000 1100 1200 1300 1500

### Questão 6

Indique a opção certa riscando a errada e justifique a sua resposta.

- a) Um computador A está a enviar um ficheiro para o computador B através de uma conexão TCP. Supondo que o computador B tem dados para enviar para A então B envia para A dois tipos de segmentos: segmentos com dados e segmentos com ACKs.

|                    |                    |
|--------------------|--------------------|
| <b>Sim, porque</b> | <b>Não, porque</b> |
|--------------------|--------------------|

- b) O tamanho do campo RevWindow do cabeçalho TCP nunca se altera durante toda a duração da conexão TCP

|                    |                    |
|--------------------|--------------------|
| <b>Sim, porque</b> | <b>Não, porque</b> |
|--------------------|--------------------|

- c) Um computador A está a enviar um ficheiro para o computador B através de uma conexão TCP. Supondo que o número de sequencia de um segmento enviado de A para B é N, então o número de sequencia do próximo segmento é necessariamente N+1.

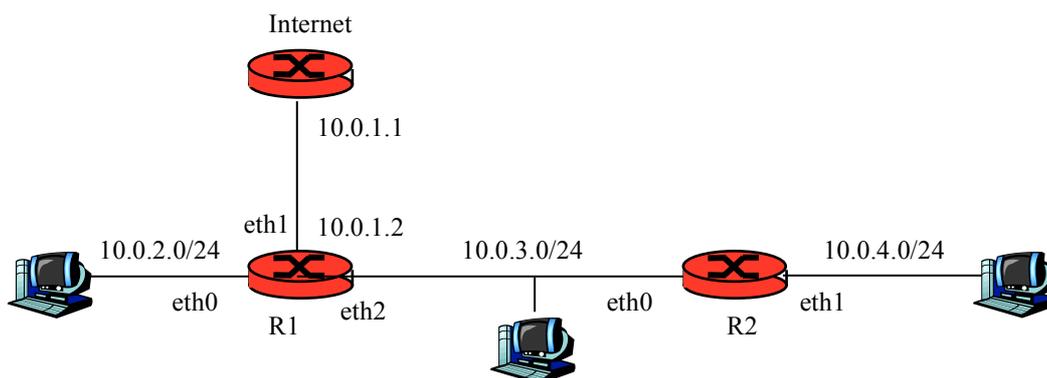
**Sim, porque**                      **Não, porque**

**Questão 7**

Na rede a seguir indicada existem várias sub-redes interligadas pelos *routers* **R1** e **R2**. O *router* **R1** por sua vez liga à Internet através de um router de um ISP que conhece pelo endereço **10.0.1.1**. Tendo em conta os endereços das redes indicados, atribua endereços a cada uma das interfaces dos routers e indique a tabela de encaminhamento do *router* R1.

**Tabela de endereços das interfaces dos routers**

|           | Eth0     | Eth1     | Eth2     |
|-----------|----------|----------|----------|
| Router R1 | 10.0.2.1 | 10.0.1.2 | 10.0.3.1 |
| Router R2 | 10.0.3.2 | 10.0.4.2 | —        |



**Tabela de encaminhamento do *router* R1**

| Prefixo IP de destino | Tipo de encaminhamento (directo, indirecto ou por defeito) | Next hop ou gateway (interface ou endereço) | Número de hops (routers) que o pacote tem de atravessar |
|-----------------------|--|---|---|
| 10.0.1.0/24           |  |   |   |
| 10.0.2.0/24           |  |   |   |
| 10.0.3.0/24           |  |   |   |
| 10.0.4.0/24           |  |   |   |
| 0.0.0.0               |  |   |   |

### Questão 8

Numa rede, os routers têm vários vizinhos, a cada um dos quais estão ligados directamente por uma interface. Por hipótese, todos os destinos existentes na rede e todos os routers são identificados por uma letra: **A, B, C, ..., Z**. As interfaces que ligam um router aos vizinhos têm por identificador a letra do vizinho.

Um router envia um pacote **p** para o vizinho **X** usando a função **sendTo ( p, X )**

Um router tem acesso ao seu identificador através do método **myID()**

Um pacote **p** tem os seguintes campos: **p.source**, **p.destination**, **p.ttl** e **p.data** com os significados óbvios.

Um router tem uma tabela de encaminhamento **rt** que suporta vários métodos, entre os quais:

- **rt.gateway ( destination )** - devolve o vizinho que encaminha para **destination** ou **null** se **rt** desconhece **destination**
- **rt.cost ( destination )** - devolve o custo do caminho deste router até **destination** ou **infinity** se **rt** desconhece **destination**
- **rt.set ( destination, gateway, cost )** - actualiza a entrada da tabela de encaminhamento referente a **destination**.

a) Escreva o pseudo código usado pelo router para processar um pacote **p** que recebeu. Se o router não sabe ou não pode processar o pacote deve ignorá-lo.

Processar o pacote **p**

b) Na rede usa-se o algoritmo Bellman-Ford para actualizar as tabelas de encaminhamento. Escreva o pseudo código usado por um router para gerar uma entrada de um anúncio sobre o destino **D** que vai enviar ao vizinho **V**. O router usa a versão “*split horizon with poison reverse*” do algoritmo.

Dado o destino **D** calcular o valor **D<sub>cost</sub>** com que o router anuncia ao vizinho **V** o destino **D** que conhece

c) Na rede usa-se o algoritmo Bellman-Ford para actualizar as tabelas de encaminhamento. Escreva o pseudo código usado por um router para processar uma entrada de um anúncio que recebeu do vizinho  $V$  à distancia  $V_{cost}$ . O vizinho comunica que conhece o destino  $D$  à distancia  $D_{cost}$ .

Processar o anúncio sobre o destino  $D$ , que o vizinho  $V$  considera à distancia  $D_{cost}$ .  $V$  está à distancia  $V_{cost}$  deste router.

d) Escreva o pseudo código usado pelo router para processar um pacote  $p$  que recebeu. Se o router não conseguir processar o pacote ignora-o mas gera um pacote *ERROR*. Inspire-se no protocolo ICMP para decidir para onde envia este pacote *ERROR*. Pode recorrer ao código da alínea a) para proceder ao envio.

Processar o pacote  $p$

### Questão 9

Com um programa de captura dos pacotes de dados (*Wireshark*) monitorizou-se o tráfego que atravessava a interface Ethernet fixa (ligação com fios) de um computador ligado a uma rede local. Nessa monitorização capturou-se o excerto de informação em anexo. Com base nessa informação responda às seguintes questões:

a) Como pode verificar, o pacote capturado no instante 4 (0.009551 s após o início da captura) diz respeito a uma interrogação DNS. O pedido foi feito por um computador, cujo endereço IP é \_\_\_\_\_ (cliente DNS), por um processo que funciona no porto \_\_\_\_\_, usando um *socket* (TCP ou UDP?) \_\_\_\_\_. Trata-se de um pedido ao servidor DNS com endereço IP \_\_\_\_\_, sendo o pedido enviado para o porto: \_\_\_\_\_, para resolver o nome DNS \_\_\_\_\_.

b) Para que serve o campo *Transaction ID* (cujo valor é 0x91aa) enviado pelo cliente na query DNS ? Justifique.

c) De acordo com a captura mostrada, torna-se claro que o pacote que transporta a *query* DNS, suportada na pilha TCP/IP, pode ser representada de acordo com o empilhamento de protocolos da seguinte figura.



c1) A que protocolos correspondem os cabeçalhos CAB1, CAB2 e CAB3 e qual o nível (na pilha TCP/IP) que cada um desses protocolos concretiza (entre o nível canal – que por hipótese inclui o nível físico e *data-link*, nível rede, nível transporte e o nível aplicação).

**CAB1:** é o cabeçalho do protocolo \_\_\_\_\_ que concretiza o nível: \_\_\_\_\_

**CAB2:** é o cabeçalho do protocolo \_\_\_\_\_ que concretiza o nível: \_\_\_\_\_

**CAB3:** é o cabeçalho do protocolo \_\_\_\_\_ que concretiza o nível: \_\_\_\_\_

c2) Dados os anteriores cabeçalhos, em que cabeçalho viaja o MAC *address* 00:06:25:26:4f:03 associado à interface de rede do computador que está a fazer o pedido DNS ? \_\_\_\_\_

c3) Em que cabeçalho viaja a informação do porto do *socket* do servidor DNS ? \_\_\_\_\_

c4) Em que cabeçalho viaja o endereço IP do computador que originou o pedido DNS ? \_\_\_\_\_

c5) Onde viaja o campo com a informação *TransactionID* respeitante ao pedido DNS ? \_\_\_\_\_

c6) Sendo o DNS um protocolo que funciona sobre IP, como é que o computador que fez o pedido obteve a informação de que o MAC *address* da interface Ethernet do servidor DNS é 00:0f:a3:90:ed:19 ?

### Questão 10

O protocolo SSL permite estabelecer um canal de comunicação seguro, entre um cliente e um servidor, sendo esse canal seguro suportado em TCP, podendo ser usado, por exemplo, para suportar interações HTTPS entre um browser e um servidor WEB.

a) Indique (**Verdadeiro - V ou Falso - F**) se as propriedades de segurança desse canal asseguram:

**P1:** Autenticação unilateral do *endpoint*/endereço IP nome DNS, de um servidor WEB acessado por HTTPS: \_\_\_\_\_

**P2:** Integridade de todos os dados nas mensagens HTTP trocadas entre o browser e o servidor: \_\_\_\_\_

**P3:** Confidencialidade de todos os dados nas mensagens HTTP trocadas entre o browser e o servidor: \_\_\_\_\_

**P4:** Confidencialidade de toda a informação do cabeçalho do protocolo TCP que suporta a conexão HTTPS: \_\_\_\_\_

**P5:** Confidencialidade de toda a informação do cabeçalho do protocolo IP que suporta a conexão TCP: \_\_\_\_\_

**P6:** Proteção contra *Denial of Service* (ou negação de serviço) na abertura da conexão TCP (nomeadamente durante o protocolo *3-handshake* de abertura da conexão TCP) entre o browser e o servidor HTTPS : \_\_\_\_\_

b) Para concretização das propriedades de segurança do canal subjacente à conexão HTTPS, o protocolo SSL usa diversos mecanismos e processos criptográficos, entre os quais:

- **M1:** Assinaturas digitais baseadas em algoritmos criptográficos assimétricos (ou de chave pública), com as chaves certificadas por certificados de chave pública emitidos por entidades (CAs) previamente reconhecidas pelo browser e pelo servidor HTTPS
- **M2:** Cifra de dados com um algoritmo criptográficos simétrico e uma chave partilhada que foi estabelecida na fase de *handshake* do protocolo SSL
- **M3:** Utilização de uma função segura de *hashing* para cálculo de sínteses de segurança dos dados que viajam nas mensagens HTTP (protegidas na conexão HTTPS).

Dadas as propriedades de segurança da alínea a), nas quais escreveu VERDADEIRO (ou V), indique qual o mecanismo que está associado ao seu suporte, preenchendo **M1**, **M2** ou **M3** na 2ª coluna da tabela. Marque X na 2ª coluna para as propriedades de segurança que entende que não são suportadas.

| Propriedades | Mecanismos |
|--------------|------------|
| <b>P1</b>    |            |
| <b>P2</b>    |            |
| <b>P3</b>    |            |
| <b>P4</b>    |            |
| <b>P5</b>    |            |
| <b>P6</b>    |            |

ANEXO

The image shows a Wireshark capture of network traffic. The main display area contains a table of captured packets. Packet 3 is selected, showing details for a Domain Name System (query) response. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time     | Source            | Destination       | Protocol | Length | Info  |
|-----|----------|-------------------|-------------------|----------|--------|---|
| 1   | 0.000000 | LinksysG_26:4f:03 | Broadcast         | ARP      | 42     | Who has 192.168.1.254? Tell 192.168.1.5         |
| 2   | 0.005540 | AlphaNet_90:ed:19 | LinksysG_26:4f:03 | ARP      | 60     | 192.168.1.254 is at 00:0f:a3:90:ed:19           |
| 3   | 0.005623 | 192.168.1.5       | 192.168.1.254     | DNS      | 77     | Standard query 0x91aa A asc.di.fct.unl.         |
| 4   | 0.009551 | 192.168.1.254     | 192.168.1.5       | DNS      | 93     | Standard query response 0x91aa A 193.136.122.33 |
| 5   | 0.012998 | 192.168.1.5       | 193.136.122.33    | TCP      | 74     | 42010 > http [SYN] Seq=0 Win=5840 Len=0         |
| 6   | 0.044565 | 193.136.122.33    | 192.168.1.5       | TCP      | 74     | http > 42010 [SYN, ACK] Seq=0 Ack=1 Win=5840    |
| 7   | 0.044768 | 192.168.1.5       | 193.136.122.33    | TCP      | 66     | 42010 > http [ACK] Seq=1 Ack=1 Win=5856         |
| 8   | 0.048543 | 192.168.1.5       | 193.136.122.33    | HTTP     | 523    | GET /rc HTTP/1.1                                |
| 9   | 0.085534 | 193.136.122.33    | 192.168.1.5       | TCP      | 66     | http > 42010 [ACK] Seq=1 Ack=458 Win=6880       |
| 10  | 0.088496 | 193.136.122.33    | 192.168.1.5       | HTTP     | 689    | HTTP/1.1 301 Moved Permanently (text/html)      |
| 11  | 0.088586 | 192.168.1.5       | 193.136.122.33    | TCP      | 66     | 42010 > http [ACK] Seq=458 Ack=624 Win=7        |
| 12  | 0.110701 | 192.168.1.5       | 193.136.122.33    | HTTP     | 524    | GET /rc/ HTTP/1.1                               |
| 13  | 0.152554 | 193.136.122.33    | 192.168.1.5       | TCP      | 1434   | [TCP segment of a reassembled PDU]              |

**Packet 3 Details:**

- Frame 3: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
- Ethernet II, Src: LinksysG\_26:4f:03 (00:06:25:26:4f:03), Dst: AlphaNet\_90:ed:19 (00:0f:a3:90:ed:19)
- Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.254 (192.168.1.254)
- User Datagram Protocol, Src Port: 41107 (41107), Dst Port: domain (53)
- Domain Name System (query)
  - Transaction ID: 0x91aa
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - asc.di.fct.unl.pt: type A, class IN

**Packet Bytes:**

```

0000  00 0f a3 90 ed 19 00 06 25 26 4f 03 08 00 45 00  .....%&O...E.
0010  00 3f 38 3c 40 00 40 11 7e 1e c0 a8 01 05 c0 a8  .78<@.@.~.....
0020  01 fe a0 93 00 35 00 2b 37 58 91 aa 01 00 00 01  ....5.+7X.....
0030  00 00 00 00 00 00 03 61 73 63 02 64 69 03 66 63  ....a sc.di.fc
0040  74 03 75 6e 6c 02 70 74 00 00 01 00 01         t.unl.pt .....
    
```

Flags (dns.flags), 2 bytes ; Packets: 165 Displayed: 165 Marked: 0 Load time: 0:00.410 ; Profile: Default