



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

Licenciatura em Engenharia Informática — Exame de Redes de Computadores
Ano lectivo: 2010/2011 – Chamada de Época Normal — (25 de Junho de 2011)
Exame sem consulta, com a duração de 2 horas e 30 minutos, 8 questões e 5 folhas

Pode-se responder a lápis mas não se podem separar as folhas umas das outras
A interpretação do enunciado faz parte da avaliação

Não se podem usar calculadores nem telemóveis durante a resolução — só papel de rascunho
Em caso de desistência deve entregar-se o exame com a menção “DESISTI”, 45 min. após o início do exame

Aluno nº _____ Nome: _____

Questão 1)

Considere as seguintes tecnologias de redes de acesso, indicadas na coluna 1 da tabela seguinte.

- a) **Classifique na coluna 2** cada uma das tecnologias da coluna 1, segundo a sua utilização, de acordo com as seguintes categorias e usando as respectivas siglas indicadas:

- AR: acesso fixo residencial
- AH: acesso fixo residencial, também utilizável por um pequeno escritório ou uma pequena empresa ou organização com menos de 5 utilizadores.
- AC: acesso fixo corporativo ou empresarial para uma grande empresa ou organização
- AM: acesso móvel.

Eventualmente pode indicar mais do que uma categoria, sempre que tal faça sentido, mas não deve ter mais do que duas siglas (AR, AC, AH ou AM) em cada célula.

- b) **Classifique na coluna 4** cada uma das tecnologias de redes de acesso da coluna 1, indicando uma taxa de transmissão característica de cada uma das tecnologias de redes de acesso apresentadas na coluna 1, de acordo com as seguintes siglas, **indicando ainda na coluna 3** se a taxa upload/download é simétrica ou assimétrica.

- TX1: 56Kbps,
- TX2: 128Kbps,
- TX3: 0.5 Mbps a 30 Mbps
- TX4: 10Mbps,
- TX5: 11Mbps,
- TX6: 56 Mbps,
- TX7: 100Mbps,
- TX8: 1000Mbps,
- TX9: 10Gbps,
- TX10: 5 a 10 Mbps.

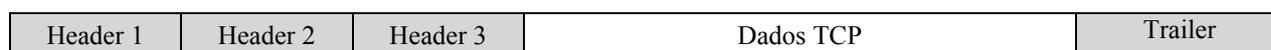
- c) De todas as tecnologias de redes de acesso referidas na coluna 1 da tabela, **indique com um “X” na coluna 5**, quais as que são de acesso partilhado e possuem um mecanismo de controlo de colisões ?

Coluna 1: Tecnologia de rede de acesso	Coluna 2: Caracterização de uso Preencher: AR, AC, AM, AH	Coluna 3: Preencher: Simétrico ou Assimétrico	Coluna 4: Taxa de transmissão de referência Preencher: TX1, TX2, ... etc, ...TX10	Coluna 5 Indicar com “X” as tecnologias de redes de acesso partilhado que requerem controlo de acesso ao meio
Acesso via Dial-Up Modem suportado numa linha telefónica analógica				
Acesso ISDN (Integrated Services Digital Network)				
Acesso “Asymmetric Digital Subscriber Line”				
Acesso do tipo HFC ou “Hybrid Fiber Coax”				
Acesso FTTH				
Switched Ethernet IEEE 802.3 na variante 100BaseT				
Ethernet IEEE 802.11b				
Ethernet IEEE 802.11g				
WiMAX IEEE 802.16				

Questão 2

Quando um pacote TCP chega a um computador por uma interface de rede Ethernet, irá ser processado sucessivamente pela pilha TCP/IP até que os dados que transporta sejam recebidos por uma aplicação.

Para o efeito, a informação dos diversos cabeçalhos associados ao processamento nos vários níveis da pilha estão representados na frame inicial que o computador recebeu na sua interface. Esta representação está indicada na figura seguinte que apresenta, nomeadamente, as zonas da frame onde viajam aqueles cabeçalhos (headers) e os dados transportados pelo segmento TCP que irá ser processado e respectivo trailer.



a) Faça corresponder os vários tipos de cabeçalhos às zonas assinaladas como 1, 2 e 3:

Headers Ethernet: corresponde ao _____

Headers TCP: corresponde ao _____

Headers IP: correspondente ao _____

b) Indique, para cada um dos campos (Headers IP, TCP ou Ethernet e Trailer) acima indicados, onde viaja a seguinte informação:

CRC-32 de verificação de erro da frame Ethernet: está contido no: _____

Endereço IP origem: está contido no _____

Número de sequência do segmento TCP: está contido no _____

Endereço MAC (Ethernet) destino: está contido no _____

Porto TCP destino: está contido no _____

Questão 3)

- a) Que protocolo de transporte na pilha TCP/IP é adoptado pelas aplicações de VOZ sobre IP (VOIP) com transmissão de áudio em tempo real, baseadas no protocolo RTP ?

Resposta: _____

- b) Indique as razões que justificam a adopção do protocolo indicado na resposta da alínea anterior a partir dos critérios e requisitos da transmissão de *streaming* suportado no protocolo RTP, em relação às seguintes propriedades:

Critério: Packet Loss (ou perda de pacotes):

> Em relação a este critério, a transmissão de áudio e vídeo *streaming* apresenta como requisito:

> Justifica-se o uso do protocolo de transporte que indico em a) para satisfação deste critério porque:

Critério: End-to-End Delay (ou tempo de latência extremo a extremo)

> Em relação a este critério a transmissão de áudio e vídeo *streaming* apresenta como requisito:

> Justifica-se o uso do protocolo de transporte que indico em a) para satisfação deste critério porque:

Critério: Packet Jitter:

> Em relação a este critério a transmissão de áudio e vídeo *streaming* apresenta como requisito:

> Justifica-se o uso do protocolo de transporte que indico em a) para satisfação deste critério porque:

Questão 4)

Considere que um computador (com IP 192.168.1.132) pretende enviar um pacote para o computador de nome pc2.mynet.com. Na sua rede existe um servidor de DNS com o IP 192.168.1.1 e um router com endereço 192.168.1.2. Descreva a sequência de pacotes **enviados e recebidos** para cada uma das alíneas seguintes, indicando se é enviado ou recebido, quais os endereços ethernet, se o protocolo é ARP ou IP e, neste último caso, qual o protocolo de transporte encapsulado no pacote IP e quais os endereços IP. Note que o computador tem na sua tabela de ARP apenas:

192.168.1.132 - c2:2a:03:00:ba:58 - eth0
192.168.1.1 - c2:c7:03:00:00:fe - eth0

a) Descreva a sequência de pacotes trocados (emitidos e recebidos) para resolver o nome:

enviado ou recebido:	Tipo do conteúdo do frame (ARP ou IP):	
Endereço ethernet origem:	Protocolo de transporte encapsulado no pacote IP:	
Endereço ethernet destino:	IP origem:	IP destino:

enviado ou recebido:	Tipo do conteúdo do frame (ARP ou IP):	
Endereço ethernet origem:	Protocolo de transporte encapsulado no pacote IP:	
Endereço ethernet destino:	IP origem:	IP destino:

a) Admita que o IP destino do pacote é 196.69.132.34. Descreva a sequência de pacotes trocados (emitidos e recebidos) para enviar este pacote:

enviado ou recebido:	Tipo do conteúdo do frame (ARP ou IP):	
Endereço ethernet origem:	Protocolo de transporte encapsulado no pacote IP:	
Endereço ethernet destino:	IP origem:	IP destino:

enviado ou recebido:	Tipo do conteúdo do frame (ARP ou IP):	
Endereço ethernet origem:	Protocolo de transporte encapsulado no pacote IP:	
Endereço ethernet destino:	IP origem:	IP destino:

enviado ou recebido:	Tipo do conteúdo do frame (ARP ou IP):	
Endereço ethernet origem:	Protocolo de transporte encapsulado no pacote IP:	
Endereço ethernet destino:	IP origem:	IP destino:

Questão 5)

Das seguintes afirmações indique VERDADEIRO ou FALSO para cada caso. Nas afirmações consideradas FALSAS justifique de forma rigorosa corrigindo a afirmação para que fique correcta, eventualmente com um contra-exemplo

a) Em HTTP e usando conexões não persistentes, não é possível que um segmento TCP possa vir a transportar como carga (payload) duas mensagens HTTP resultantes de dois pedidos.

b) Para um browser descarregar por HTTP 1.1 as páginas <http://www.di.fct.unl.pt/index.html> , <http://www.di.fct.unl.pt:80/image1.gif> e <http://asc.di.fct.unl.pt/>, necessitará de as receber através de duas conexões persistentes.

- c) Pretendendo-se descarregar um objecto por HTTP através de um browser WEB, não sendo esse objecto uma página com referências a outros objectos, do ponto de vista de desempenho é indiferente usar HTTP/1.0 ou HTTP/1.1 com ou sem *pipelining*.

- d) Usando HTTP 1.1 para aceder a uma página WEB com um conteúdo HTML que inclui três imagens (GIF), para o browser conseguir mostrar a página e as imagens, poderá fazer um único pedido HTTP e receber quatro mensagens de resposta HTTP, usando sempre a mesma conexão.

- e) Para se enviar uma frame Ethernet que transporta um pacote IP numa rede com endereço 10.20.30.0/24 destinado ao endereço 235.55.22.19, será preciso usar o protocolo ARP para obter o endereço MAC associado ao endereço destino.

- f) Para se enviar uma frame Ethernet que transporta um pacote IP numa rede com endereço 10.20.30.0/24 destinado ao endereço 10.20.30.255/24, não será preciso usar o protocolo ARP para obter o endereço MAC associado ao endereço destino.

- g) O protocolo TCP utiliza ao nível dos seus mecanismos de controlo e recuperação de percas de pacotes apenas os mecanismos fundamentais inspirados no protocolo do tipo SELECTIVE REPEAT.

- h) Num protocolo do tipo GO-BACK-N o receptor nunca confirma a boa recepção de pacotes cujos números de sequencia não sejam o do pacotes esperado.

- i) O valor do campo RcvWindow que viaja no cabeçalho de qualquer segmento TCP nunca pode ter o valor zero, durante uma conexão TCP.

- j) No protocolo de encaminhamento do tipo Distance Vector, a técnica de anunciar rotas com adição de *Poisoned Reverse* evitará sempre a possibilidade de ocorrência de ciclos no encaminhamento de pacotes, devido ao problema da contagem até ao infinito.

Questão 6)

Apresente em pseudo código o tratamento realizado por um *router* a um pacote *p* que recebeu pela interface *i*, sabendo que o *router* está a usar um algoritmo de encaminhamento por inundação.

a) O *router* tem as interfaces i_1, i_2, \dots, i_N . *p.origin* e *p.destination* dão acesso aos endereços origem e destino do pacote. *p.ttl* ao seu TTL. *p.register ()* regista o endereço origem do pacote e um seu identificador numa tabela de pacotes já vistos. *p.isDuplicate ()* devolve um booleano indicando se o pacote recebido é ou não um duplicado. *p.transmit (interface i)* transmite o pacote *p* pela interface *i* e *p.flood (interface i)* transmite o pacote *p* por todas as interfaces excepto *i*.

```
void floodPacket ( packet p, interface i) {
```

```
}
```

b) Considere o algoritmo de aprendizagem utilizado pelos *switches* Ethernet. Inspirando-se nesse algoritmo proceda a uma optimização do algoritmo que anteriormente propõe em a), consistindo a optimização em ter uma tabela de encaminhamento *TR* que regista a interface que está na origem de um caminho para um destino. Essa tabela é actualizada sempre que o *router* recebe um pacote que não é um duplicado. Considere que dispõe das seguintes funções para utilização no seu algoritmo optimizado:

TR.putRoutingEntry (address a, interface i) regista que o destino *a* está acessível via a interface *i* substituindo qualquer associação anterior de *a* a qualquer outra interface.

TR.getRoutingEntry (address a) devolve a interface por detrás da qual está o endereço destino *a* ou devolve null se o mesmo endereço não está na tabela.

```
void processPacket ( packet p, interface i) {
```

```
}
```


Questão 8)

Escolha uma das seguintes questões (8 – Opção A ou 8 – Opção B) para responder.

Note que só pode responder a uma delas.

Questão 8 na OPÇÃO B

Questão para responder a partir do contexto do capítulo de redes wireless e redes 802.11

a) Suponha que uma estação receptora (*Base Station ou Access Point*) operando o protocolo IEEE 802.11b está configurada para gestão de CSMA-CA usando o mecanismo RTS/CTS.

Suponha que um computador ligado a essa estação base, num dado instante através de uma interface 802.11b, precisa de transmitir uma frame de dados de dimensão igual a 11000 bits para um computador que também se encontra associado através de uma interface 802.11b à mesma estação base e que o meio físico está livre quando o computador emissor começa a tentar detectar se há colisões no momento.

De acordo com a definição das seguintes slots temporais associadas ao processamento 802.11, ignorando o tempo de propagação, assumindo que não haverá erros, e considerado que o tempo de transmissão de frames RTS e CTS é dado por $TS=0,1$ ms, indique, justificando, qual o tempo mínimo expectável para que a interface wireless do computador emissor possa dar a frame como tendo sido recebida pelo receptor.

SIFS: Short Interface Space Time = 20 microsegundos para redes 802.11b

DIFS: DFS Interframe Space = 50 microsegundos para redes 802.11b

b) Repita o cálculo e verifique qual o ganho no envio da mesma frame, se a estação base e os computadores estiverem a usar interfaces segundo a norma 802.11g, sabendo que:

SIFS: Short Interface Space Time = 9 a 20 microsegundos para redes 802.11g

DIFS: DFS Interframe Space = 28 a 50 microsegundos para redes 802.11g

Questão 8)

Escolha uma das seguintes questões (8 – Opção A ou 8 – Opção B) para responder.

Note que só pode responder a uma delas.

Questão 8 na OPÇÃO B

Questão para responder a partir do contexto do capítulo de Segurança

- a) De acordo com o seu conhecimento do campo CRC no processamento uma frame ethernet, acha que o cálculo do valor desse CRC, nos moldes em que é feito, poderia ser substituído por uma função segura de Hashing ? Que vantagens e desvantagens teria ? Justifique a resposta.

- b) O protocolo de *Needham-Schroeder* para distribuição e estabelecimento de chaves criptográficas simétricas está resumido na seguinte troca de mensagens, utilizando-se a notação habitual associada à apresentação deste protocolo, no que diz respeito ao conteúdo das mensagens e processamentos criptográficos relevantes.

Complete a informação que falta, de acordo com o seu conhecimento do protocolo, que permite a A e B passarem a estabelecer uma chave de sessão K_s que podem utilizar depois da mensagem 4.

1: A>KDC A, B N_{1a}

2: KDC>A { N_{1a} , B, K_s , {A, K_s , T_a } K_b } K_a

3: A>B { N_{2a} } K_s , _____

4: B>A { _____ } K_s

KDC: Key Distribution Center

K_a : Chave criptográfica simétrica de longa duração, partilhada entre A e KDC

K_b : Chave criptográfica simétrica de longa duração, partilhada entre B e KDC

N_i : Nonce gerado pela entidade i (por ex., N_{1a} é um nonce N_1 gerado por A)

T_a : Timestamp gerado por A

T_b : Timestamp gerado por B

K_s : Chave de sessão a estabelecer entre A e B

S: I > K: mensagem enviada de I para K (com número de ordem de sequencia indicado em S)

Notar que as vírgulas representam concatenações das partes indicadas nas mensagens