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

Licenciatura em Engenharia Informática — Exame de Redes de Computadores
Ano lectivo: 2008-2009 – Chamada de Recurso — (20 de Julho de 2009)
Exame sem consulta, com 11 questões e com a duração de 2 horas e 30 minutos

Pode-se responder a lápis mas não se podem separar as folhas umas das outras
A interpretação do enunciado faz parte da avaliação
Se vem levantar a nota escreva "MELHORIA" no campo superior direito
Não se podem usar calculadoras nem telemóveis durante a resolução — só papel de rascunho

Aluno nº _____ Nome: _____

1) Usando o programa *ping*, mediu-se repetidamente durante 100 segundos o tempo de trânsito (ida e volta ou RTT) de pacotes de 100 bytes entre dois hosts ligados através de uma rede de pacotes e verificou-se que os valores medidos varia entre 10 ms e 300 ms com um valor médio de 50 ms e uma variância elevada. Justifique o que está na origem c comportamento? O mesmo seria possível numa rede de circuitos ?

A variância elevada deve-se ao facto de, numa conexão feita numa rede de pacotes, ser possível que os pacotes enviados percorram sempre caminhos diferentes, passando por diferentes routers e canais. Em cada router um pacote sofre atrasos de vários tipos (tempo em fila de espera, tempo de processa tempo de transmissão e propagação) que causam a variância verificada nos resulta do ping.
Numa rede de circuitos não existe tanta variância porque os pacotes são encaminhados por um caminho estabelecido entre hosts, que se mantém sempre ao longo da conexão

2) O computador A está ligado a um *router* R (que funciona em *store & forward*) por um canal com 5 mili segundos de tempo de propagação e 1 Mbps de velocidade de transmissão. O *router* R liga-se a um computador B através de um canal também com 5 mili segundos de tempo de propagação e 1 Mbps de velocidade de transmissão. Qual a taxa de utilização do canal que liga A a R (isto é, a percentagem do tempo em que o computador A está efectivamente a transmitir através desse canal) por um protocolo do tipo "stop & wait", que utiliza mensagens com 10.000 bits de comprimento para transmitir um ficheiro de A para B, admitindo que não há erros e desprezando o tempo de transmissão dos ACKs. A resposta só está certa com contas indicadas e certas.

Tempo de transmissão de cada pacote: $T_t = \frac{\text{Dim. pacote}}{\text{Vel. Trans}} = \frac{10^4 \text{ bits}}{10^6 \text{ bps}} = 0{,}01\text{ s} \; (= 10\text{ms})$

Cada pacote leva a transitar de A para B: (stop'n'wait)

$T_{total} = T_{tAR} + T_{pAR} + T_{tRB} + T_{pRB} + \underbrace{2T_p}_{ACK} = 0{,}01 + 0{,}005 + 0{,}01 + 0{,}005 + 2\times 0{,}005 = 0{,}04\text{ s} \; (= 40\text{ms})$

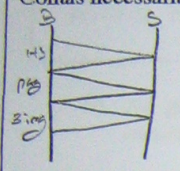
$T_U = \frac{0{,}01}{0{,}04} = 25\%$

Taxa de utilização (%) = 1 5 10 15 17 20 22 (25) 30 33 45 50 80 100% outro valor diferente destes

0,01 é o tempo que o emissor passa a transmitir
0,04 é o tempo total para um pacote

3) Um cliente HTTP acede a uma página HTML num servidor. Depois de obter essa página, o cliente deduz que a mesma tem 3 imagens e que as mesmas devem ser obtidas igualmente, a partir desse mesmo servidor, para mostrar o conteúdo total ao utilizador. O tempo de trânsito ida e volta (RTT) entre o cliente e o servidor é de 100 mili segundos. O cliente não tem nenhuma conexão aberta para o servidor antes de aceder à página mas já conhece o seu endereço IP. O tempo necessário para transmitir os pacotes com os comandos, a página ou as imagens são negligenciáveis. Qual o menor tempo necessário para obter a página e as imagens usando o protocolo HTTP 1.1 **com** *pipelining* ?

Contas necessárias:



$T_f = 3 \times RTT = 3 \times 100 = 300\ ms$

Tempo total em ms = 100 200 (300) 350 400 450 500 600 700 800 900 950 1000 1100 1200 1300 1400 1500 1600 1700 1800 1900 2000 nenhum destes valores

4) Admita que todos os telefones móveis de Portugal (cujos números começam pelo dígito "9" e têm sempre 9 dígitos) passavam a ter um endereço IP associado.

a) Foi proposto usar a seguinte solução para registar esses endereços IP no DNS: cada telefone móvel passaria a ser conhecido por um nome DNS da forma: número-telefone.mobile.pt. Exemplo: 915678927.mobile.pt. Analise esta solução.

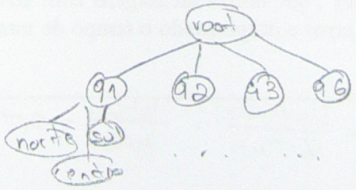
Problema / ~~vantagem~~ 1: Servidor centralizado (mobile.pt) é fonte de problemas e ataques.

Problema / ~~vantagem~~ 2: Queries todas direccionadas para o mesmo sítio, o que pode levar a um nível de tráfego muito elevado.

~~Problema~~ / vantagem 3: Ponto conhecido com informação sobre os números telemóvel

b) Proponha uma alternativa, continuando a usar o DNS, que permita uma gestão descentralizada do domínio.

Uma alternativa seria dividir os números por vários DNS, escalados por operadora e dentro desses poderia-se também dividir os números por DNS locais às regiões.



5) Quais das seguintes questões são verdadeiras ou falsas. A sua resposta tem de ser justificada. Assinale claramente a opção que escolher como certa.

a) As páginas "asc.di.fct.unl.pt/index.html" e "asc.di.fct.unl.pt/rc/index.html" podem ser transmitidas pela mesma conexão TCP usando o protocolo HTTP 1.1.

Sim, porque com ~~Não, porque~~
o protocolo HTTP 1.1 é possível manter a conexão activa para vários pedidos, desde que os pedidos sejam feitos ao mesmo servidor (o que também se verifica neste caso).

b) As páginas "www.fct.unl.pt/index.html" e "asc.di.fct.unl.pt/index.html" podem ser transmitidas pela mesma conexão TCP usando o protocolo HTTP 1.1.

~~Sim, porque~~ Não, porque não se encontram no mesmo servidor, o que obriga a fechar a conexão após o primeiro pedido para depois voltar a abrir-la com outro servidor.

c) Com conexões persistentes HTTP 1.1 é impossível que um único segmento TCP transporte duas mensagens HTTP distintas.

Sim, porque ~~Não, porque~~

6) Suponha que o ISP "big-isp.pt" recebe grandes quantidades de correio electrónico dirigido aos seus clientes. Os utilizadores do ISP têm endereços de correio electrónico da forma "user@big-isp.pt". O ISP tem 3 servidores de correio electrónico: "big1.big-isp.pt", "big2.big-isp.pt" e "big3.big-isp.pt". Explique que outras entradas DNS o domínio "big-isp.pt" precisa de ter para que as mensagens de correio electrónico que são dirigidas aos utilizadores do ISP sejam distribuídas equitativamente pelos seus 3 servidores. Justifique a sua resposta.

Big1.big-isp.pt	IN	A	193.136.122.100
Big2.big-isp.pt	IN	A	193.136.122.200
Big2.big-isp.pt	IN	A	193.136.122.250

7) Um computador A está a transferir um ficheiro muito grande para um computador B, usando uma ligação TCP, através da Internet. O canal *bottleneck* atravessado pelos pacotes trocados pelos dois computadores tem a velocidade de transmissão de 1 Mbps disponível para a ligação TCP entre os dois. O RTT médio entre A e B é de 10 ms (mili segundos). Constata-se, durante a transferência do ficheiro, que o protocolo TCP está sempre na sua fase de *congestion avoidance*, pois está a detectar a perca de pacotes, quando tenta ultrapassar a capacidade do canal *bottleneck*, através do mecanismo designado por *fast retransmit*. Qual a capacidade média dessa ligação TCP medida de extremo a extremo entre A e B? Apresente as contas e justifique o resultado.

$T_s = 1\,Mbps = 1000\,Kbps$

$RTT = 10\,ms$

como varia constantemente entre $\frac{W}{2}$ e $W \Rightarrow 0{,}75 \times \frac{W}{RTT}$

$0{,}75 \times 1000 / \ldots = 750\,Kbps$

Capacidade média em Kbps = 100 200 300 350 400 450 500 550 600 650 700 (750) 800 850 900 950 1000 1100 1200 1300 1400 1500 1600 1700 1800 1900 2000 nenhum destes valores

8) Responda verdadeiro ou falso às seguintes questões justificando sumariamente a sua resposta. Assinale claramente a opção que escolher como certa.

a) Com a versão "repetição selectiva" do protocolo de janela deslizante é possível o emissor receber um ACK sobre um pacote que cai fora da sua janela de emissão.

~~Sim, porque~~ Não, porque enquanto um pacote não tiver o seu ACK confirmado não é removido da janela de emissão, de maneira a ser possível re-enviar esse pacote em caso de perda do mesmo.

b) Com a versão "Go-back-N" do protocolo de janela deslizante é possível o emissor receber um ACK sobre um pacote que cai fora da sua janela de emissão.

igual...

~~Sim, porque~~ Não, porque

c) O protocolo "stop & wait" é o mesmo que o protocolo de janela deslizante na versão "repetição selectiva" com o emissor e o receptor com janelas de dimensão 1.

~~Sim, porque~~ Não, porque o receptor não guarda os pacotes que recebe fora de ordem.

d) O protocolo "stop & wait" é o mesmo que o protocolo de janela deslizante na versão "Go-back-N" com o emissor e o receptor com janelas de dimensão 1.

Sim, porque ~~Não, porque~~

9) Um computador tem uma interface Ethernet (eth0) com o endereço IP 192.168.1.5. Admita também que as suas tabelas de ARP e de encaminhamento IP têm o seguinte conteúdo:

ARP:

192.168.1.1	23:45:A0:4F:67:CD
192.168.1.5	23:45:AB:2F:67:AD
192.168.1.10	23:45:AB:2F:60:CD

Encaminhamento IP:

192.168.1.0/24	directo eth0
default	router 192.168.1.254

a) Indique os endereços origem, destino e respectivo tipo do(s) *frame(s)* Ethernet que o computador deve enviar pela interface eth0 para encaminhar um pacote com endereço IP de destino 192.168.1.10.

Tipo do conteúdo do frame 1:
Endereço origem: 23:45:AB:2F:67:AD
Endereço destino: 23:45:AB:2F:60:CD

Tipo do conteúdo do frame 2:
Endereço origem:
Endereço destino:

Tipo do conteúdo do frame 3:
Endereço origem:
Endereço destino:

b) Indique os endereços origem, destino e respectivo tipo do(s) *frame(s)* Ethernet que o computador deve enviar pela interface eth0 para encaminhar um pacote com endereço IP de destino 192.168.1.150.

Tipo do conteúdo do frame 1:
Endereço origem:
Endereço destino:

Tipo do conteúdo do frame 2:
Endereço origem:
Endereço destino:

Tipo do conteúdo do frame 3:
Endereço origem:
Endereço destino:

c) Indique os endereços origem, destino e respectivo tipo do(s) *frame(s)* Ethernet que o computador deve enviar pela interface eth0 para encaminhar um pacote com endereço IP de destino 190.130.120.45.

Tipo do conteúdo do frame 1:
Endereço origem:
Endereço destino:

Tipo do conteúdo do frame 2:
Endereço origem:
Endereço destino:

Tipo do conteúdo do frame 3:
Endereço origem:
Endereço destino:

10) Um *switch* Ethernet, com as portas p_1, p_2, ..., p_N recebe um *frame f* pela porta *p*. ***f.source*** e ***f.dest*** dão acesso aos endereços MAC (Medium Access Control) origem e destino do *frame f*. A tabela de filtragem ***ft*** do *switch* é acessível pelos seguintes métodos: ***ft.getRoute(address mac)*** que devolve a porta por detrás da qual está a estação com endereço MAC ***mac*** ou *null* se a mesma não é conhecida ou se o tempo de permanência de ***mac*** em ***ft*** está esgotado, e ***ft.storeRoute (port p, address mac)*** que associa a estação com endereço ***mac*** à porta porta *p*, esmagando qualquer associação anterior. ***f.send (port p)*** transmite o *frame f* pela porta *p* e ***f.flood (port p)*** transmite o *frame f* por todas as portas excepto *p*. Escreva o pseudo código do algoritmo de processamento dos frames recebidos pelo *switch*.

```
void processFrame ( frame f, port p) {




}
```

11) No último encontro que tiveram, a Alice e o Bob partilharam uma **chave** secreta **simétrica**, $\mathbf{K_{AB}}$. Porém, eles só querem usar essa chave, $\mathbf{K_{AB}}$ esporadicamente devido ao seu receio dela vir ser apanhada por um atacante.

Descreva um protocolo que permita à Alice interagir com o Bob nos seguintes termos:

i) A Alice quer enviar uma mensagem **em claro** ao Bob, assinada por ela. Ou seja, o conteúdo da mensagem não é confidencial, mas o Bob deverá poder **comprovar** que foi a Alice que a enviou.

ii) A Alice pretende no seguimento da mensagem anterior receber uma resposta do Bob, **confidencial**, que deverá, ainda, dar provas que o Bob **leu a mensagem** anterior e que foi o **Bob que respondeu**.

Nota: Utilize a notação apropriada para indicar o formato das mensagens trocadas pelo protocolo que desenvolveu.

Alice ---- $M, \{M, N_A, K_S\}_{K_{AB}}$ ----→ Bob

Bob ---- $\{N_A, N_S\}_{K_S}$ ----→ Alice

Complete a sua resposta, descrevendo os símbolos usados nas mensagens, como indicado para $\mathbf{K_{AB}}$.

$\mathbf{K_{AB}}$ - chave simétrica partilhada pela Alice e o Bob.