

Nome: _____ N°: _____
Nome: _____ N°: _____

Ficha Prática Nº 1

Conceitos de Sistemas Informáticos: 2005/06

Ligue a sua máquina e introduza o login **diguest** e a senha **diguest**. Seleccione a opção **Linux fedora 4 <net>** e espere que o sistema operativo seja carregado. Entre no login **diguest** com a senha **diguest** e depois faça **startx** para activar o ambiente gráfico X Window.

A seguir são apresentadas uma série de questões. Uma vez respondidas, o aluno deverá devolver a ficha ao docente da disciplina a fim de ser avaliada.

1. Com auxílio do **man**, investigue os comandos **hostname** e **/sbin/ifconfig**. Diga qual é o nome completo da sua máquina (opção **-f**) e os respectivos endereços de hardware, de Internet, de broadcast, e a máscara de rede associada.

Uma rede Internet permite a troca de informação entre os computadores que a constituem. Para tal, a informação é transportada em vários pacotes contendo os dados da aplicação e os cabeçalhos adicionados pelos diversos protocolos das camadas da pilha TCP/IP. O **ethereal** é uma aplicação de captura de tráfego que permite analisar o conteúdo dos pacotes que circulam numa rede.

Faça **su** – e depois introduza **diguest** como password de root. Invoque o **ethereal** e capture alguns pacotes. Observe os pacotes capturados e escolha um que contenha dados de aplicação.

2. A figura que se segue representa um pacote Ethernet completo, com os vários cabeçalhos protocolares encapsulados. Complete-a indicando os protocolos que observa encapsulados no seu pacote e o tamanho respectivo de cada um dos cabeçalhos protocolares.

(preâmbulo)	Lig. Lógica	Rede	Transporte	Aplicação	(CRC)
8 bytes	Prot _____ Tam _____	Prot _____ Tam _____	Prot _____ Tam _____	Prot _____	4 bytes

3. Presentes no seu pacote deverão estar 4 endereços distintos: dois endereços físicos presentes no cabeçalho Ethernet e dois endereços de rede presentes no cabeçalho IP. Identifique-os e transcreva-os, e determine o tamanho (em bytes) de um endereço ethernet e de um endereço IPv4. Diga ainda, justificando, se o pacote analisado foi recebido ou emitido pela sua máquina.

4. Ao contrário de um endereço físico, um endereço IP é constituído por dois campos: um que define a (sub)rede a que diz respeito e outro que identifica a máquina nessa mesma rede. A máscara de rede permite identificar os bits respeitantes à (sub)rede.

Identifique o endereço IP da sua máquina na representação do pacote em hexadecimal que observa na janela inferior, e converta-o para binário. Aplique-lhe a máscara de rede fazendo um AND lógico bit-a-bit, e, auxiliando-se das tabelas de conversão, apresente em decimal as componentes de rede e de host obtidas.

Bin	Dec	Hex
0000	= 0	= 0
0001	= 1	= 1
0010	= 2	= 2
0011	= 3	= 3
0100	= 4	= 4

Bin	Dec	Hex
0101	= 5	= 5
0110	= 6	= 6
0111	= 7	= 7
1000	= 8	= 8
1001	= 9	= 9

1010	= 10	= a
1011	= 11	= b
1100	= 12	= c
1101	= 13	= d
1110	= 14	= e
1111	= 15	= f

5. As máquinas pertencentes à mesma subrede têm o mesmo prefixo de rede IP. Máquinas pertencentes a redes IP diferentes deverão comunicar através de equipamentos especiais chamados routers. Assim sendo, diga, justificando, se o pacote em análise passou por algum router.

6. O endereço IP de broadcast é reservado para enviar mensagens a todas as máquinas existentes na rede IP a que diz respeito. Observando o endereço de broadcast da sua máquina, deduza como se constrói um a partir do endereço de rede.

7. Investigue o comando **ping**. Como usaria este comando para saber rapidamente o endereço IP de todas as máquinas activas existentes na sua rede IP?

8. O número de porta, existente nos cabeçalhos de transporte, permite identificar o protocolo de aplicação envolvido numa comunicação. Identifique as portas origem e destino presentes no pacote em análise. Com ajuda do `vi /etc/services`, determine a porta atribuída aos serviços http e smtp (email).

9. Pretende-se aceder por http à máquina servidora **marco** existente no domínio **uminho.pt** para obter a página **index.html** existente na directoria <directoria-base das pág. html>/disciplinas/CSI. Indique a URL respeitante a este recurso, e confirme-a com o seu *browser*.

Os filtros do ethereal permitem capturar (*capture filter*) ou mostrar (*display filter*) apenas pacotes com características específicas. Apesar de ambos filtros produzirem o mesmo *output* final, existem diferenças essenciais nos fins a que se destinam. A captura de tráfego com visualização em tempo real é o exemplo típico da utilização do *capture filter*.

Na sua máquina arranque um *browser* (e.g. netscape, mozilla) e configure-o para utilizar o *proxy* HTTP **proxy.di.uminho.pt** (193.136.19.6, 193.136.19.8) na porta **3128** (Edit > Preferences > Proxies > ...).

10. Coloque o ethereal a capturar tráfego. Com o browser da sua máquina aceda à página indicada na alínea anterior, e depois pare a captura.

a) Porque razão os pacotes que trazem a página pretendida não provêm nem da máquina marco.uminho.pt, (193.136.9.240) nem da porta 80 (atribuída ao serviço http)? Qual a máquina e a porta de que é proveniente a página? A que máquina o seu browser efectuou o pedido http?

b) Transcreva a regra que permite ao *display filter* (Analyze>Display Filter) mostrar unicamente pacotes cujo endereço IP destino seja o da sua máquina, e cujo nº de porta origem seja o da proxy. Experimente-a com os pacotes capturados na alínea anterior.

11. Coloque novamente o ethereal a capturar tráfego, mas agora com o *capture filter* especificado para a regra da alínea anterior. Com o *browser* da sua máquina volte a aceder à mesma página (com Shift+Reload), e depois pare a captura.

a) Transcreva a especificação usada no filtro, e diga, observando a captura, quantos ficheiros foram transferidos para a sua máquina ao aceder à referida página?

b) Quantos pacotes foram precisos para transferir o código html da página, e qual o tamanho total deste? (sugestão: procurar esta informação no campo Content-Length presente no cabeçalho da resposta HTTP)

c) Qual a percentagem de bytes imposto pelo protocolo de comunicação TCP/IP relativamente à quantidade de bytes do código html transferido, ou seja, qual é o *overhead* imposto pelo TCP/IP nessa transferência?

Nota: adicione 12 bytes a cada cabeçalho ethernet, por forma a contabilizar o preâmbulo e o campo de verificação de erros CRC.