universidade de aveiro
theoria poiesis praxis

Redes e Serviços

Objetivos

- Verificação da configuração de rede de um PC
- Tradução de nomes para endereços IP e vice-versa
- Testes de conectividade
- Familiarização com o analisador de protocolos WireShark
- Estudo do protocolo ICMP

Duração

1 aula

Verificação da configuração de rede

1. Abra uma janela de linha de comandos (terminal).

2. No terminal execute os seguintes comandos (em Linux):

```
ifconfig
route -n
cat /etc/resolv.conf
```

e registe: (i) quantos interfaces de rede existem, (ii) o endereço IP de cada um dos interfaces, (iii) o(s) *default gateway(s)*, (iv) o endereço físico de cada um dos interfaces e (v) o endereço IP dos servidores de DNS.
Nota 1: Execute os comandos `man ifconfig` e `man route` para obter a ajuda/manual dos comandos `ifconfig` e `route`. O comando `man` pode ser usado com qualquer outro comando disponível em linha de comandos.
Nota 2: o ficheiro `/etc/resolv.conf` contem a listagem dos serviudores de DNS (nameserver) e o comando `cat` lista o conteúdo de um ficheiro.

Windows 10
Pressione Win+X para abrir o menu contextual e clique na opção *Prompt de Comando* (Admin).

```
ipconfig
route print
```

Tradução de nomes para endereços IP e vice-versa

3. Numa janela de comandos, utilizando o comando `host` determine o(s) endereço(s) IP associado(s) aos nomes das máquinas na tabela abaixo. Identifique os nomes com mais do que um endereço IP associado e quais os nomes que têm o mesmo endereço IP associado. O que conclui?
Nota: Em alternativa pode usar os comandos `nslookup` ou `dig`.

Nome	Endereço(s) IP
www.ua.pt	
ua.pt	
www.up.pt	
www.tvi.iol.pt	
www.sapo.pt	
www.tsf.pt	
www.clix.pt	
www.antena3.pt	
www.rtp.pt	
www.publico.pt	
www.publico.clix.pt	
www.google.com	
www.google.pt	
www.google.es	

4. Dos endereços IP obtidos na experiência anterior escolha 4 e utilizando o comando `host` (`nslookup`) determine o nome associado a esses endereços IP. Relacione os resultados obtidos com os resultados da experiência anterior, o que conclui?

Endereço IP	Nome

5. Faça a resolução para endereço IP dos seguintes nomes. Abra o *browser* e coloque na barra de endereço os nomes e os endereços IP. O que conclui?

Nomes	Endereço IP
www.up.pt	
www.sapo.pt	
www.rtp.pt	
www.antena3.pt	
cnn.com	
ac360.com	

Testes de conectividade

6. Numa janela de comandos, execute o comando `ping` para os seguintes endereços e registe o tempo médio de ida e volta (*rtt avg*). O que pode concluir relativamente à relação existente entre o tempo médio de ida e volta e a distância geográfica?

Endereços	Localização da máquina	Tempo médio de ida e volta
www.ua.pt	Aveiro, Portugal	
www.up.pt	Porto, Portugal	
www.ul.pt	Lisboa, Portugal	
www.utad.pt	Vila Real, Portugal	
www.uevora.pt	Évora, Portugal	
www.uam.es	Madrid, Espanha	
www.univ-paris8.fr	Paris, França	
www.cmu.edu	EUA	
www.zju.edu.cn	China	
www.u-tokyo.ac.jp	Tóquio, Japão	
www.adelaide.edu.au	Austrália	

Descoberta de percursos entre a origem e o destino

7. Execute o comando `tracepath` (`tracert` em windows) para os seguintes endereços e registe o número de máquinas de rede entre a origem e o destino e o endereço da antepenúltima máquina desse percurso.
Nota 1: Poderá usar em alternativa o comando `traceroute`.
Nota 2: Algumas máquinas do percurso entre a origem e destino não poderão ser identificadas porque estão configuradas para não responder a este tipo de pacotes ou os pacotes estão a ser bloqueados por uma *firewall* no percurso.
Nota 3: O *trace route* para um destino poderá ser feito através de um serviço web (ex: http://ping.eu/), no entanto a origem será sempre o servidor onde este serviço web está localizado.

Endereços	Localização da máquina	Número de máquinas
www.ua.pt	Aveiro, Portugal	
www.up.pt	Porto, Portugal	
www.fc.ul.pt	Lisboa, Portugal	
www.utad.pt	Vila Real, Portugal	
www.uevora.pt	Évora, Portugal	
www.uam.es	Madrid, Espanha	
www.univ-paris8.fr	Paris, França	
www.cmu.edu	EUA	
www.zju.edu.cn	China	
www.u-tokyo.ac.jp	Tóquio, Japão	
www.adelaide.edu.au	Austrália	

Descoberta da entidade responsável pelas máquinas de rede

8. Utilizando o serviço *whois,* a partir da página http://whois.domaintools.com/,determine (se possível), para cada um dos *trace routes* efetuados na experiência anterior: a entidade responsável por algumas das máquinas de cada um dos percursos e a localização geográfica dessa entidade.

Endereço IP	Entidade responsável	Localização da entidade

9. Utilizando o serviço *whois,* a partir da página http://www.domaintools.com/,determine as entidades responsáveis por alguns dos nomes Internet da experiência 3 e pelos respetivos endereços IP.

Nome	Endereço IP	Entidade responsável pelo nome	Entidade responsável pelo endereço IP

Familiarização com o analisador de protocolos

10. Execute a aplicação *wireshark*. Com o objectivo de capturar todos os pacotes que chegam ao interface de rede da sua máquina: (i) aceda ao menu Capture⇒Options..., (ii) active a opção "*Capture packets in promiscuous mode*" e (iii) certifique-se que o campo "C*apture filter*" está em branco. Inicie a captura clicando em "*Start"*, aceda à página www.ua.pt e prolongue a captura por 30 segundos. Termine a captura acedendo ao menu Capture⇒Stop. Identifique os pacotes IP capturados e os seus endereços IP de origem e destino.

11. Na janela principal do *wireshark*, defina um filtro de visualização para pacotes do protocolo HTTP introduzindo **http** no campo "*filter*" e clicando em "*Apply*".
Inicie a captura clicando em Capture⇒Start, aceda à página www.ua.pt e prolongue a captura por 30 segundos. Termine a captura acedendo ao menu Capture⇒Stop. Identifique os pacotes HTTP capturados e os seus endereços IP de origem e destino.

12. Na janela principal do *wireshark*, defina um filtro de visualização para pacotes do protocolo HTTP com origem ou destino na sua máquina introduzindo
ip.addr == *<endereço IP>* && http no campo "*filter*" e clicando em "*Apply*". O campo ***<endereço IP>*** deverá ser substituído pelo endereço IP da sua máquina. Inicie a captura clicando em Capture⇒Start, aceda à página www.ua.pt e prolongue a captura por 30 segundos. Termine a captura acedendo ao menu Capture⇒Stop. Identifique os pacotes HTTP capturados e os seus endereços IP de origem e destino.

Protocolo ICMP

14. Na janela principal do *wireshark*, defina um filtro de visualização para pacotes do protocolo ICMP (ping) com origem ou destino na sua máquina introduzindo
ip.addr == *<endereço IP>* && icmp no campo "*filter*" e clicando em "*Apply*". O campo ***<endereço IP>*** deverá ser substituído pelo endereço IP da sua máquina. Inicie a captura clicando em Capture⇒Start. Execute os seguintes comandos:

(i) *ping* www.ua.pt
(ii) *ping* -c 2 www.av.it.pt (*ping -n* 2 www.av.it.pt)
(iii) *ping* -s 256 www.ieeta.pt (*ping* -l 256 www.ieeta.pt)

Termine a captura acedendo ao menu Capture⇒Stop. Identifique os pacotes ICMP capturados, os seus endereços IP de origem e destino, o tipo de pacote (campo *info*) e o tamanho de cada pacote.