Trabalho TEÓRICO/PRÁTICO 4

Configurações e Testes de Rede, Protocolos e Serviços de Rede

Docente: Mário Jorge Pina da Fonseca Pinto

Discente: 127111 - Douglas cancella nunes lobo

05.05.2025

# índice

[índice 2](#_Toc197469364)

[Parte 1 – configuraçsão de rede 3](#_Toc197469365)

[Minha máquina 3](#_Toc197469366)

[Meu servidor 5](#_Toc197469367)

[Parte 2 – definição de endereços ip 7](#_Toc197469368)

[Concepção da rede 7](#_Toc197469369)

[parte 3 – resolução de endereços 9](#_Toc197469370)

[Tabela ARP e como verificar-lhe as entradas 9](#_Toc197469371)

[Como adicionar entradas à tabela ARP 11](#_Toc197469372)

[Como deletar entradas da tabela ARP 11](#_Toc197469373)

[Como descobrir o endereço IP e MAC do seu Gateway 11](#_Toc197469374)

[parte 4 – teste de ligação de rede 13](#_Toc197469375)

[parte 5 – dhcp e dns 17](#_Toc197469376)

[DHCP 17](#_Toc197469377)

[DNS 20](#_Toc197469378)

[Whois 23](#_Toc197469379)

# Parte 1 – configuraçsão de rede

## Minha máquina

De antemão deixo claro que não usei algumas ferrementas sugeridas pelo professor por conta do meu sistema – que é um macOS –, portanto, ainda que tenha alguns portes instalados pelo gestor Homebrew, preteri-os em favor das ferramentas nativas, nomeadamente: netstat, ifconfig, arp, route, scutil, ipconfig e networksetup.

Recolhi as seguintes informações sobre a minha rede e máquina:

* Nome da minha interface: en0;
* Endereço MAC da minha máquina: f4:d4:88:87:41:76;
* Endereço IPv4 da minha máquina: 192.168.1.128;
* Máscara de rede da minha rede: 255.255.254.0;
* Máscara de rede (CIDR): /23 (23 bits);
* Gateway da minha rede: 192.168.1.1;
* Endereço de Broadcast da minha rede: 192.168.1.255;
* Endereço dos meus namerservers:
  + 2a01:f:3000:8::1;
  + 2a01:f:1:8::1;
  + 192.168.1.1.

Através do comando “ifconfig en0” — sendo en0 a designação da minha placa de rede no macOS, que mesmo estando conectada via Wi-Fi é tratada como uma interface Ethernet — obtive as seguintes informações:

A screen shot of a computer program

AI-generated content may be incorrect.

Através dos comandos “scutil --dns | grep nameserver | sort --unique” e “scutil --dns | head” obtive as seguintes informações:

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Através do comando “route get default” obtive as seguintes informações:

A screen shot of a computer

AI-generated content may be incorrect.

Por fim, através do comando “netstat -rn” obtive as seguintes informações:

A screenshot of a computer

AI-generated content may be incorrect.

Utilizando a ferramenta Wireshark OUI Lookup Tool com o endereço MAC da minha máquina obtive “F4:D4:88 Apple, Inc.”. Pesquisando descobri que o primeiros três bytes de um endereço MAC é reservado a identificar a fabricante pelo Organizationally Unique Identifier (OUI, que é atribuído por organizações como a Institute of Electrical and Electronics Engineers (IEEE)), sendo a minha máquina um MacBook faz sentido os três bytes iniciais do meu dispositivo corresponderem ao fabricante Apple, Inc.

## Meu servidor

Recentemente, decidi me aventurar no mundo do Home Lab. Aproveitei uma máquina que estava acumulando poeira aqui em casa e instalei o Ubuntu Server nela. Como parte da exploração, estabeleci uma conexão SSH com autenticação por chaves criptografadas (Ed25519). A seguir, reitero o processo que fiz anteriormente e, agora, com o meu servidor em uso, recolhi as seguintes informações sobre a máquina:

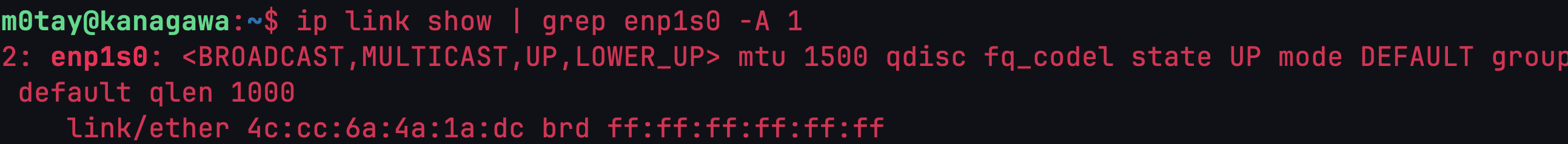
* Nome do servidor: kanagawa;
* Nome da interface do servidor: enp1s0 (agora sim é realmente Ethernet);
* Endereço MAC do servidor: 4c:cc:6a:4a:1a:dc;
* Endereço IPv4 do servidor: 192.168.1.133;
* Máscara de rede da minha rede: 255.255.254.0;
* Máscara de rede (CIDR): /23 (23 bits);
* Gateway da minha rede: 192.168.1.1;
* Endereço de Broadcast da minha rede: 192.168.1.255;
* Endereço dos seus namerservers:
  + 2a01:f:3000:8::1;
  + 2a01:f:1:8::1;
  + 192.168.1.1.

Através do comando “ip a | grep enp1s0 -A 5” obtive as seguintes informações:

A screenshot of a computer program

AI-generated content may be incorrect.

Através do comando “ip link show | grep enp1s0 -A 1” obtive as seguintes informações:



Através do comando “ip route” obtive as seguintes informações:

A screen shot of a computer

AI-generated content may be incorrect.

Através do comando “resolvectl status” obtive as seguintes informações:

A screen shot of a computer

AI-generated content may be incorrect.

Utilizando a ferramenta Wireshark OUI Lookup Tool com o endereço MAC do meu servidor obtive “4C:CC:6A Micro-Star INTL CO., LTD.” o que está correto.

# Parte 2 – definição de endereços ip

## Concepção da rede

Uma empresa necessita de criar uma rede informática com capacidade para acomodar os atuais 220 equipamentos e ter uma margem de 25% de crescimento para acrescentar novos equipamentos no futuro.

Com base no requerimento do professor, onde devo conceber uma rede no molde 10.A.B.0, com A sendo 127 e B sendo 11 — os primeiros três e os dois últimos dígitos do meu número mecanográfico, respetivamente — proponho a rede 10.127.10.0/23\*.

De momento, a empresa possui 220 equipamentos. Considerando uma margem de crescimento de 25%, chegamos a um total de 275 dispositivos. Uma máscara /24 (255.255.255.0) oferece apenas 254 endereços válidos, o que não seria suficiente. Assim, proponho uma máscara /23 (255.255.254.0), que fornece 510 endereços válidos — mais que o dobro do necessário —, garantindo margem de crescimento e organização. Proponho as seguintes configurações para essa rede:

* Endereço de Rede: 10.127.10.0;
* Máscara de Rede: 255.255.254.0;
* Endereço de Broadcast: 10.127.11.255;
* Primeiro Endereço IP: 10.127.10.1;
* Último Endereço IP10.127.11.254;
* Número de Hosts possíveis: 510;
* Endereços IP fixos a atribuir: 19;

\*Nota: Mesmo que eu tenha partido do endereço 10.127.11.0, como a máscara escolhida é 255.255.254.0 (/23), isso faz com que a rede comece, na verdade, em 10.127.10.0. Pesquisando descobri que isso acontece porque essa máscara agrupa dois blocos de endereços consecutivos, ou seja, cobre de 10.127.10.0 até 10.127.11.255. É um detalhe técnico, mas importante para garantir que os endereços usados estejam dentro da faixa certa. Isso é, ainda que eu diga que a rede é 10.127.11.0, ela continuará ocupando os dois blocos de 10.127.10.0 até 10.127.11.255. Portanto, irei fazer esse pequeno ajuste, ainda que fira a premissa do professor. Segue-se um desenho que pode ajudar a clarificar o meu raciocínio, primeiro desenho o problema e depois porque fui *forçado* a escolher outra rede:

A diagram of a network

AI-generated content may be incorrect. A diagram of a network

AI-generated content may be incorrect. Em suma o que esses desenhos evidenciam é que o primeiro bit do terceiro octeto é tratado como um bit pertencente aos hosts e não aos bits da network. Achei muito interessante entender porque que em toda calculadora de IP que acessava e introduzia a rede 10.127.11.0/23 ele me dizia que o gama da network seria de 10.127.10.1-10.127.11.254.

# parte 3 – resolução de endereços

## Tabela ARP e como verificar-lhe as entradas

O protocolo ARP funciona uma interface entre duas camadas do modelo OSI: a segunda e terceira camada. Entre minhas pesquisas cheguei a encontrar gente a chamá-lo de protocolo da camada 2.5. O seu funcionamento consiste em descobrir o endereço MAC associado a um dado IP dentro de uma rede (LAN). Com efeito, é criada uma tabela onde esses pares são registrados. Através do comando “arp -a” ter-se-á um resultado como ouput parecido com esse:

A screen shot of a computer

AI-generated content may be incorrect.

Tomemos uma entrada como exemplo: “? (192.168.1.133) at 4c:cc:6a:4a:1a:dc on en0 ifscope [ethernet]”. Interpretamos a linha deste modo: entre parênteses se encontra o IP do dispositivo (meu servidor); “at 4c:cc:6a:4a:1a:dc” indica o endereço MAC do meu servidor; “on en0” indica que essa entrada foi observada na interface de rede “en0”, que comumente é a interface Wi-Fi de um Mac, como já abordei anteriormente; “ifscope [ethernet]” apenas reforça o dado anterior.

A screen shot of a computer

AI-generated content may be incorrect.

O meu servidor tem acesso a outros dispositivos, imagino por estar realmente conectado à rede através de um cabo ethernet.

Pesquisando também sobre os possíveis estados na tabela ARP e decidi experimentar como seria ter uma entrada e interagir com ela no estado “noarp”:

A computer screen shot of a program

AI-generated content may be incorrect.

Com o recurso dos pontos:

1. O comando enviado ao terminal adiciona um IP “192.168.1.200” inexistente na rede com um endereço MAC “00:11:22:33:44:55” forjado para a camada de ligação de dados na interface da rede “enp1s0” e declara-lhe o estado como “permanent”;
2. Imprimo a tabela ARP, o dispositivo forjado está ali;
3. Simulo “pingar” o dispositivo, com efeito, como este não existe não recebe os pacotes;
4. Deleto o IP forjado;
5. Imprimo a tabela arp, o dispositivo forjado não se encontra mais entre os reais.

Através do comando “arp -ali en0” obtive as seguintes informações:

A screen shot of a computer screen

AI-generated content may be incorrect.

As flags “-i (mais o argumento ‘en0’)” e “-l” foram usadas para apresentar mais informações relevantes e de num output em tabela, como indica o comando “man arp”:

A screen shot of a computer

AI-generated content may be incorrect.

## Como adicionar entradas à tabela ARP

Para adicionar entradas à tabela usa-se o comando “sudo arp -s <ip> <mac>”, onde <ip> é o hostname que iremos adicionar à tabela e <mac> o endereço MAC daquele dispositivo. Através desse comando obtive esse resultado:

A screen shot of a computer

AI-generated content may be incorrect.

## Como deletar entradas da tabela ARP

Para deletar entradas da tabela usa-se o comando “sudo arp -d <ip>”, onde <ip> é o hostname que iremos deletar da tabela. Através desse comando obtive esse resultado:

## Como descobrir o endereço IP e MAC do seu Gateway

Para descobrir o endereço IP usa-se o comando “route get default”, que faz um lookup da rota padrão utilizada pelo sistema, revelando o gateway (roteador) e a interface de saída “en0”. Depois recorremos ao comando “arp <ip>” para vermos a entrada que corresponde ao <ip> provido.

Interpretando as informações obtemos o gateway que é 192.168.1.1 que coincide com o endereço IP do meu router; e vendo na tabela ARP especificando aquele IP temos que o endereço MAC do meu router é d0:cf:e:5b:3a:47.

A black screen with red and green text

AI-generated content may be incorrect.

# parte 4 – teste de ligação de rede

Para testar a minha ligação de rede irei fazer de início um ping ao sapo.pt, para testar e analisar a minha conectividade à internet, através do comando “ping -c 4 sapo.pt”, onde “-c 4” indica uma quantidade de pings por efetuar, por padrão é até ser parada a execução do comando e o último argumento “sapo.pt” é o meu alvo:

A screenshot of a computer screen

AI-generated content may be incorrect.

Com o recurso dos pontos, interpretemos o output:

1. Nessa linha vemos que o domínio “sapo.pt” foi resolvido para “213.13.146.142” e que cada pacote ICMP tem um payload de 56 bytes;
2. Nas seguintes, vemos a sequência de 4 respostas, onde “64 bytes” indica o tamanho da resposta recebida, “from 213.13.146.142” indica o IP que respondeu, “icmp\_seq=<n>” indica o número sequencial dos pacotes (útil para debug), “ttl=<n>” não nos interessa aqui, e “time=<t> ms” indica a latência — ou seja, o tempo de ida e volta, em milissegundos;
3. Nas últimas linhas, vemos que todos os pacotes transmitidos chegaram e voltaram, com 0% de perda de pacotes, e por fim, o comando mostra a latência mínima, média e máxima.

O posso concluir a partir dessas informações é que a ligação com sapo.pt está funcionando. A latência está baixa e estável, o que condiz com o fato de estarmos no mesmo país.

Através do comando “traceroute -m 8 sapo.pt” obtive a rota que os pacotes seguem desde o meu equipamento até ao servidor de destino, no caso, sapo.pt. “-m 8>” indica a quantidade de hops (saltos) limite. É enviado um pacote de 40 bytes para o endereço de IP 213 .13.146.142. Guiando-se pela numeração dos saltos: o primeiro salto é para o meu gateway (router); o segundo salto é provavelmente para o meu ISP (NOS) e mostra o DNS; das linhas para frente os asteriscos indicam tempo excedido ou sem resposta, por quais possíveis razões? Os intermediários não responderam ou houve perda de pacotes. Mesmo sem conseguir visualizar os saltos seguintes, eles existem, como se comprova pelo facto de o domínio ter sido resolvido com sucesso para um IP.

A computer screen with red text

AI-generated content may be incorrect.

Através do comando “traceroute ventraip.com.au” obtive a rota que os pacotes seguem desde o meu equipamento até ao servidor de destino, no caso, ventraip.com.au (103.42.108.26).

Guiando-me pela numeração dos saltos: o primeiro salto é para o meu gateway (router); o segundo salto é provavelmente para o meu ISP (NOS), com resolução de nome para um domínio da Optimus. Os saltos 3 e 4 não deram resposta, o que pode indicar roteadores configurados para ignorar pacotes ICMP ou perda temporária de pacotes. A partir do 5º salto, vejo o tráfego a passar por diversos roteadores da Cogentco, uma operadora de backbone global. Notam-se localizações como Marselha (mrs02) e Singapura (sin01), o que faz sentido dada a rota para a Austrália, penso eu. A latência aumenta gradualmente à medida que os pacotes percorrem longas distâncias intercontinentais. A partir do 12º salto, os pacotes entram na rede Superloop, uma operadora australiana. Finalmente, no 18º salto, os pacotes atingem o servidor de destino com latências na casa dos 409 ms, o que é esperado considerando a distância física e a complexidade da rota.

A existência de saltos sem resposta (asteriscos) não significa que os pacotes foram perdidos, apenas que esses eles não enviaram resposta ao traceroute. Mesmo assim, a rota completa foi alcançada com sucesso.

A screenshot of a computer screen

AI-generated content may be incorrect.

Através do comando “traceroute www.iij.ad.jp” obtive a rota que os pacotes seguem desde o meu equipamento até ao servidor de destino, neste caso, www.iij.ad.jp. O domínio foi resolvido para o endereço IP 202.232.2.180.

Guiando-se pela numeração dos saltos: o primeiro salto vai até ao meu gateway (router); o segundo para o ISP (NOS), como mostra o domínio reverso. Nos saltos 3 e 4 aparecem apenas astericos. A partir do 5º salto, vemos claramente o tráfego a atravessar a backbone da Cogentco. O tempo de resposta vai aumentando conforme a distância cresce — reflexo natural da latência em conexões transcontinentais. No 16º salto, vemos a entrada no território japonês através do domínio iij.net, e finalmente no 18º salto, o pacote chega ao destino. A latência final ronda os 300-400 ms, o que é esperado dado o percurso longo entre Portugal e o Japão.

Mesmo com algumas lacunas na rota (asteriscos), os pacotes chegaram ao destino, provando que os saltos seguintes existiram e funcionaram — apenas não foram visíveis.

A screenshot of a computer screen

AI-generated content may be incorrect.

# parte 5 – dhcp e dns

## DHCP

O DHCP é o protocolo que associa IPs a dispositivos que se conectam à rede através de uma sequência requisições enviadas entre si até que o dispositivo receba o endereço IP.

Através do comando “ipconfig getpacket en0” obtive as seguintes informações:

A screenshot of a computer program

AI-generated content may be incorrect.

Através do comando “sudo tcpdump -v -i en0 port 67 or port 68 -n”, que escuta o tráfego nas portas usadas pelo protocolo DHCP, consegui observar o momento em que o meu dispositivo solicitou uma lease (Request) e o servidor respondeu com a concessão da lease (ACK). No pacote de resposta foi possível identificar o endereço IP atribuído (192.168.1.134), o servidor DHCP (192.168.1.1), a duração da lease (3600 segundos), o gateway (192.168.1.1) e o servidor DNS (também 192.168.1.1). Esse método é útil para visualizar em tempo real a negociação da lease DHCP entre cliente e servidor, já que no macOS informações sobre DHCP são escarsas.

A screenshot of a computer program

AI-generated content may be incorrect.

Eu tentei efutuar a request de um novo lease e isso ocorreu:

A screenshot of a computer

AI-generated content may be incorrect.

Concluo que até onde pude compreender pelas minhas pesquisas que em macOS alterar o DHCP é um processo incerto: algumas vezes altera-se, outras não.

## DNS

Através do comando “dig [www.ua.pt](http://www.ua.pt)” obtive as seguintes informações:

Através do comando “nslookup www.ua.pt” retornou um "nome canônico" para o domínio, que é lvs-ng.ua.pt, e o endereço IP associado a ele é 193.136.173.58. Isso significa que o domínio [www.ua.pt](http://www.ua.pt) é redirecionado para lvs-ng.ua.pt (uma forma de alias ou CNAME, ou seja, o nome canônico) que resolve para o IP 193.136.173.58. O DNS da OpenDNS forneceu uma resposta não autoritativa, indicando que o nome foi resolvido por meio de uma consulta que não é diretamente controlada pelo servidor.

A computer screen with numbers and a number on it

AI-generated content may be incorrect.

Similar ao primeiro caso, o domínio `elearning.ua.pt` é resolvido para um nome canônico, `elearningvip.ua.pt`, com o endereço IP 193.136.173.95. O DNS da OpenDNS retornou uma resposta não autoritativa, indicando que o nome do domínio é um alias para outro nome, o qual é resolvido para o IP mencionado.

A computer screen with red text

AI-generated content may be incorrect.

Aqui o comando retornou um erro de NXDOMAIN o que significa que o domínio printing.ua.pt não foi encontrado no servidor DNS da OpenDNS. Isso pode indicar que o domínio não existe ou não está configurado corretamente para resolução públicaou que há um problema com o servidor DNS consultado.

A black background with red text

AI-generated content may be incorrect.

Por fim, através do comando “nslookup www.sapo.pt” retornou a resolução correta, com o endereço IP 213.13.146.142. O DNS da OpenDNS forneceu uma resposta não autoritativa, mas foi capaz de resolver o domínio sem problemas, confirmando que o domínio está ativo e acessível.

A screenshot of a computer code

AI-generated content may be incorrect.

A maioria dos domínios foi resolvida corretamente com a OpenDNS, exceto “printing.ua.pt”, que não foi encontrado. A resposta "não autoritativa" indica que a resolução foi feita por meio de um servidor DNS que não é o servidor autoritativo para os domínios, mas que conseguiu fornecer a resposta com base em informações armazenadas em cache ou consultas anteriores.

Os servidores NS do domínio "ua.pt" são "ns.ua.pt" e "ns2.ua.pt", enquanto os do domínio "sapo.pt" são "ns.sapo.pt", "ns2.sapo.pt", "dns01.sapo.pt" e "dns02.sapo.pt". Esses servidores são responsáveis por responder pelas zonas DNS dos respetivos domínios. Usei o comando "dig ua.pt NS +short" e "dig sapo.pt NS +short" para obter esses dados.

A screen shot of a computer

AI-generated content may be incorrect.

Usei os comandos "dig ua.pt MX +short" e "dig sapo.pt MX +short" para obter os servidores de email dos dois domínios. Para "ua.pt", obtive três servidores: "mx1.ua.pt", "mx4.ua.pt" e "mx.sapo.pt", todos com prioridade 5, o que indica que eles são usados de forma equivalente para receção de emails. Esses servidores são responsáveis por tratar o correio eletrónico do domínio.

A black screen with red text

AI-generated content may be incorrect.

Usei o comando "dig ANY" para obter todas as informações disponíveis publicamente nos servidores DNS dos domínios. Para "ua.pt", consegui vários tipos de registros: TXT (incluindo SPF e validações de serviços como Adobe e OneTrust), SOA (com info sobre a autoridade da zona), MX (servidores de email) e NS (servidores de nomes). Já para "sapo.pt", o servidor DNS respondeu apenas com os registros NS, o que indica uma política mais restritiva quanto ao tipo de informação que este disponibiliza publicamente.

A screenshot of a computer program

AI-generated content may be incorrect.

## Whois

Como o comando “whois ua.pt” retornou um output de texto como muito extenso irei enviar em anexo o txt contendo-o. Foi possível ver os dados de registro do domínio: entidade responsável, contactos administrativos, técnico, e datas de criação e expiração. Essa informação é útil para saber quem administra o domínio e quando ele foi criado, mas também sei que há websites que anonimizaram essas informações.