

**Pràctica 1. Introducció a les comunicacions**

Óscar Jiménez, NIUB: 20100286

Laurentiu Nedelcu, NIUB: 20081585

**ÍNDEX**

**OBJECTIUS 3**

**PREGUNTES I RESPOSTES 3**

[Visualització de la xarxa 3](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.5d806ws93u07)

[Verificació del protocol intern del PC](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.crzqx03chanx) 5

[Verificació de la connexió amb l’exterior 6](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.2kxm2ep0hxpx)

[Coneixement de l’entorn proper](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.lgv78ifiisg6) 7

[Estadística de xarxa](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.1tuo80u67pc2) 7

[Telnet](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.xrmn4akrvwf6) 8

[Ssh](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.44mu3x8ozske)  9

FTP 11

[**FEINA REALITZADA AL LABORATORI 1**](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.72z8cz9l4ubq)**6**

[**CONCLUSIONS**](https://docs.google.com/document/d/1Wq5XMNz_VZJfR5JjHB4klBwJaK5V7ap5rSuMeDiet3g/edit#heading=h.7vxlbpfwy6yg) **17**

**OBJECTIUS**

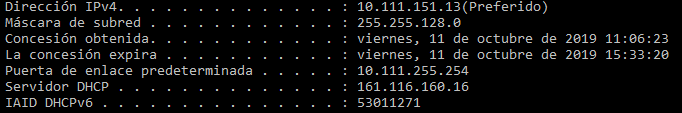
L’objectiu principal d’aquesta pràctica és conèixer i familiaritzar-nos amb les comandes que ens són d’utilitat per tal de treballar amb les xarxes d’ordinadors. En el nostre cas aprendrem a usar aquestes comandes en els sistemes operatius: Windows i Linux. Al final, amb els coneixements adquirits durant tota la pràctica hauríem de ser capaços de crear un programa que consta en un xat entre nosaltres.

**PREGUNTES I RESPOSTES**

**Visualització de la xarxa**

**Sabem la IP del nostre router?**

Si escrivim la comanda ipconfig/all podrem observar que el servidor DHCP conté la direcció IP del nostre router (161.116.160.16).



**Quina és la vostra IP? Identifiqueu si la IP que surt en el vostre PC és pública o privada fent una cerca a Internet i indiqueu quines IPs són privades.**

La nostra IP com es pot veure en la imatge superior és 10.111.151.13, la qual és una IP privada ja que està dins de l’interval 10.0.0.0 a 10.255.255.255 (que està reservada per Internet Assigned Numbers Authority (IANA)). Les IPs privades es poden veure en la següent pregunta.

**Hi ha un protocol que s’encarrega de “traduir” la IP privada en una IP pública. Aquest protocol s’anomena NAT. Busqueu la definició de NAT i expliqueu breument com funciona.**

El protocol Network Address Translation (NAT) és un mecanisme utilitzat per routers IP per intercanviar paquets entre dues xarxes que s’assignen mútuament adreces incompatibles.

Aquest protocol permet que un únic dispositiu, com un router, actuï com a agent entre una xarxa pública (Internet) i una xarxa privada (xarxa local), la qual cosa fa que només es necessiti una única adreça IP per representar tot un grup d’ordinadors. Per tant, quan els ordinadors i servidors es volen comunicar entre si, s’han d’identificar els uns als altres amb una única adreça.

Primerament, hem de saber que es va introduir una sèrie d’adreces privades que qualsevol pot utilitzar, sempre i quan es mantenen privades i no s’encaminen a Internet. Aquestes adreces privades són:

Classe A 10.0.0.0 - 10.255.255.255

Classe B 172.16.0.0 - 172.31.255.255

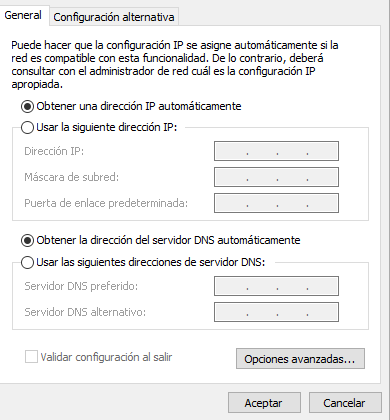
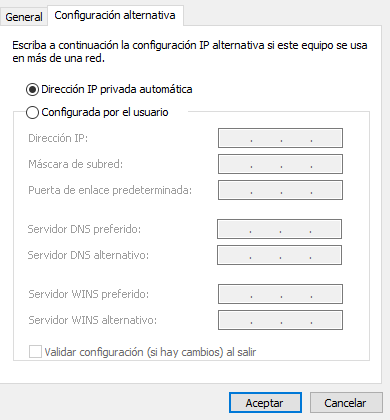
Classe C 192.168.0.0 - 192.168.255.255

NAT permet utilitzar aquestes adreces IP privades a la xarxa interna. D’aquesta manera, dins de la xarxa privada d’una empresa hi ha assignada una adreça IP única a tots els equips i una altra empresa també pot utilitzar la mateixa IP privada, sempre i quan es mantinguin interns a la seva xarxa. Per tant, dues empreses poden utilitzar el mateix rang d’adreces IP, però com que són privades a la seva xarxa, no entren en conflicte entre elles.

Tanmateix, quan els hosts interns necessiten comunicar-se amb la xarxa pública (Internet), llavors s’usaria l’adreça pública la qual representa la nostra passarel·la de xarxa. Aquesta adreça seria única i ningú més la faria servir.

Per tant, quan un host de la xarxa interna amb una adreça IP interna necessita comunicar-se fora de la seva xarxa privada, usaria l’adreça IP pública de la porta d’entrada de la xarxa per tal d’identificar-se a la resta del món i d’aquesta traducció (convertir l’adreça IP privada en pública) s’encarregaria el NAT.

**En funció del router que ens proporciona la IP, és possible també que aquesta sigui volàtil. Doneu una ullada al panel de control, i busqueu com teniu configurada la vostra IP. Descriviu breument el que trobeu.**



El que podem veure és que la nostra adreça IP és volàtil ja que tenim seleccionat la opció de que ens obtingui una adreça IP automàticament.

**En cas que la IP sigui volàtil provarem d’alliberar la IP actual. Per tal de fer això fem: ipconfig /release**

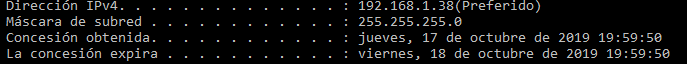
**Què ens indica ara la comanda ipconfig /all? Tornem a demanar al router una nova IP: ipconfig /renew all**

**torneu a fer ipconfig /all i constateu si s’ha canviat la vostra ip o bé manteniu encara la que ja teníeu.**

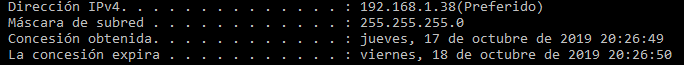
El ipconfig /all ens mostra tota la informació detallada dels valors de configuració de red TCP/IP actuals.

Després d’haver fet el release i el renew seguim mantenint la nostra direcció IP. Abans de donar la explicació, hem de saber que quan el nostre ordinador envia una sol·licitud al DHCP per tal de obtindré una adreça IP, aquest li atorga una adreça IP vàlida per un determinat nombre d’hores. Ara l’ordinador sap quina direcció IP ha d’utilitzar i per quant de temps. Després d’haver passat la meitat de les hores que se li ha adjudicat, llavors torna a fer una sol·licitud per tal d’augmentar el temps permès per a usar la direcció IP. Aquestes accions de renovació no acostumen a canviar la nostra direcció IP, és a dir, seguim usant la mateixa per un termini més llarg.

Un servidor DHCP sol tenir un llistat d’adreces IPs per tal de lliurar al nostre ordinador. La majoria solen recordar l’adreça que li ha lliurat a l’ordinador. Per tant, encara que haguéssim fet un release de la nostra adreça, el DHCP se’n recorda i normalment ens torna a donar la mateixa direcció IP quan tornem a sol·licitar una de nova. El que sí que canvia quan fem el renew és el temps del qual hem estat parlant. Com es pot observar en les imatges inferiors la nostra adreça IP no canvia, però el temps d’expiració sí.



*Informació detallada de la nostra adreça IP abans d’haver fet el release i el renew.*



*Informació detallada de la nostra adreça IP després d’haver fet el release i el renew.*

**Verificació del protocol intern del PC**

**Desconnecteu ara la vostra connexió a la LAN. Torneu a executar la instrucció. Què passa?**

El PING (Packet Internet Groper), tal com el seu nom indica, és un cercador de paquets en xarxes. Si desconnectem la nostra connexió de la xarxa local, llavors no podrem enviar els paquets a la xarxa pública, en altres paraules, els paquets es perdran.

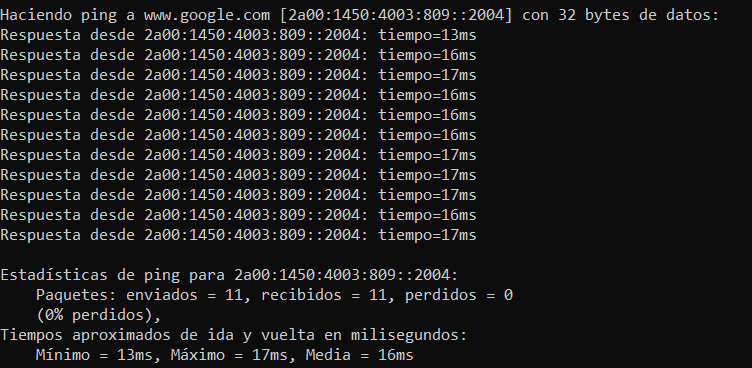
**Sense connectar el cable, executeu ara el següent: ping 127.0.0.1 Expliqueu breument que és el que heu fet i que és aquesta IP.**

Encara que no estiguem connectats a internet aquesta direcció ip és accessible, ja que aquesta apunta al nostre propi ordinador, es diu que és el “localhost”, que és la direcció IP de loopback, i és la ruta que ens permet arribar des de el nostre ordinador/servidor a nosaltres mateixos, per poder accedir als components o serveis que el nostre ordinador dona.

**Verificació de la connexió amb l’exterior**

**Verifiqueu que teniu resposta amb google. Quan triguen els paquets en fer tota la ruta completa (enviar ECO a google i detectar el retorn)?**

Els paquets triguen en fer la ruta uns 16ms de mitja, això depèn molt de la teva connexió i variarà en funció de com estiguis connectat a internet, si per cable o per WiFi, i si es connecta amb l’exterior amb ADSL o Fibra.



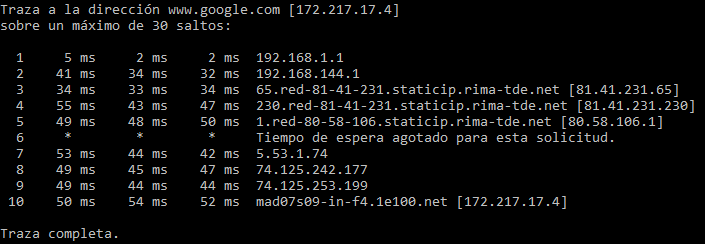
Retorn de la comanda ping www.google.com -t

**Indiqueu per quines adreces públiques circulen els datagrames. Apareix el símbol “\*”? Que indica?**

La comanda tracert utilitza el valor TTL que indica la vida màxima del paquet a la xarxa, de forma que el que busca són les respostes en les diferents profunditats per on passa el paquet abans d’arribar al destí que seria [www.google.com](http://www.google.com).

D’aquesta forma la comanda augmenta en una unitat la vida del paquet a la xarxa per a cada iteració que hi fa, i a cada una de les iteracions aconseguirà la resposta en profunditat major, i més propera al destí.

És possible que la comanda tracert ens digui que en una de les iteracions no ha pogut obtenir resposta i ho indica amb el símbol “\*”, això pot venir donat per molts factors, pot ser per un “firewall” que no deixa passar o retornar aquesta informació, o podria ser perquè la teva connexió no es trobi en “idle”, és a dir que estigui ocupada amb altres paquets i ajorni aquesta operació el suficient com per detectar que ha esperat massa temps per una resposta. Si ens fixem podem veure que el temps que triga a cada iteració no es consistent entre els diferents intents que fa tracert, i es degut a aquest fenomen.

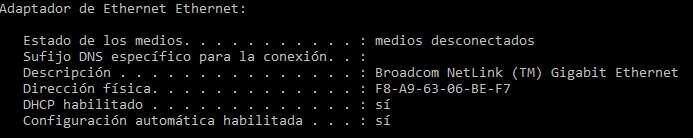


Retorn de la comanda tracert www.google.com

**Coneixement de l’entorn proper**

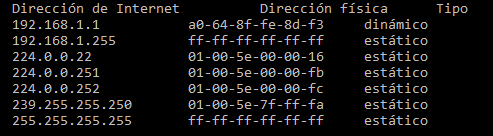
**Feu servir la comanda ipconfig per identificar la vostra adreça MAC. Quants bits té?**

La nostra adreça física és F8-A9-63-06-BE-F7, la qual té un total de 48 bits (6 blocs de dos caràcters hexadecimals, 8 bits).



**Quantes entrades té la vostra taula ARP?**

La nostra taula ARP té un total de 7 entrades, de les quals una és dinàmica i les altres són estàtiques.



**Proveu d’esborrar tota la taula ARP. Què passa? Torneu a obrir la consola i determineu la mac del router de sortida.**

Quan estem intentant esborrar totes les entrades de la taula ARP, el que estem fent en realitat és eliminar la caché. Això si, tan aviat com es fan les connexions de xarxa, la memòria cau ARP es tornarà a reconstruir. El benefici de esborrar una entrada és que de vegades una entrada ARP incorrecta pot causar problemes amb les connexions a Internet i la càrrega de pàgines web. Per tant, esborrem la memòria cau ARP i esperem a que es reconstrueixi.

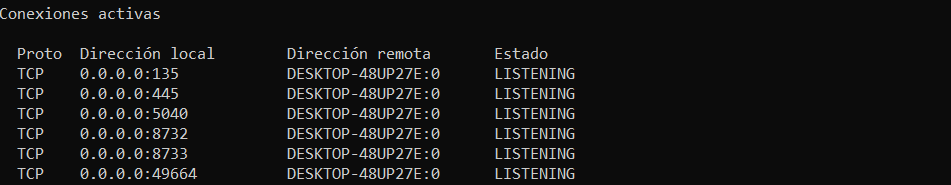
La MAC del router no canvia, segueix sent la mateixa (a0-64-8f-fe-8d-f3). L’únic que s’haurà d’esperar una mica a que es torni a crear la entrada.

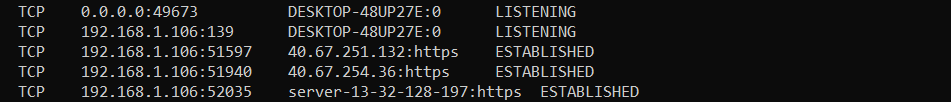
**Estadística de xarxa**

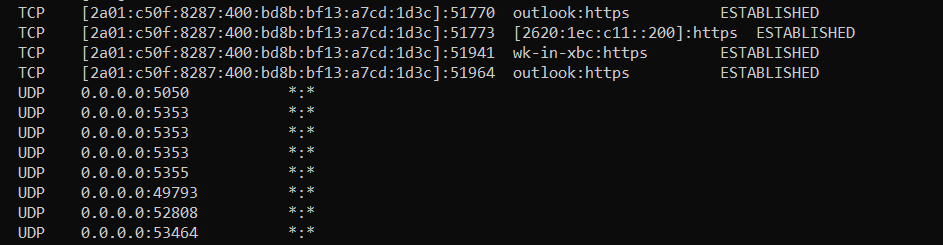
**Que fa la opció nestat –r? Que és la mètrica?**

L'opció nestat -r mostra la taula d’enrutament, que és un fitxer que ens mostra les rutes amb les connexions conegudes o actives, i aquestes rutes es tenen com a referència com a les més ràpides per arribar a un objectiu.

La taula comanda ens mostra el protocol utilitzat a cada connexió, la direcció local i la remota (direcció per la què es coneixen a l’ordinador local, i com es coneixen fora a la xarxa), i l’estat de cadascuna (establerta, escoltant ...).







Parts de la sortida de la comanda “netstat -r” que mostra les diferents tipus de connexió

**Telnet**

**Connecteu-vos amb el següent servidor: towel.blinkenlights.nl. Que fa?**

El client de telnet ens accepta el text en brut d’un servidor i el mostra, i envia les pulsacions del nostre teclat de nou al servidor.

Hem vist que el que fa la connexió a aquest servidor es mostrar una representació de la pel·lícula “Star Wars, Episode VI: A new hope” en text ASCII.

Podem trobar la animació a <http://asciimation.co.nz/>.

**Ssh**

Fent servir dos ordinadors amb ubuntu18.04 LTS una distribució de linux, hem fet servir un com a servidor i l’altre de client. Per poder utilitzar les comandes relacionades amb “net”, hem hagut de instal·lar net-Tools amb la comanda:

sudo apt install net-tools

Després de fer-ho als dos ordinadors, és necessari saber quina es la ip de l'ordinador que utilitzarem com a servidor, i llavors executar al client la comanda:

ssh -X usuariHost@IP\_host

On “usuariHost” seria el nom d’usuari del compte que utilitza el servidor, seguit de la ip del servidor. Però si ho fem sense obrir d’alguna forma un servidor al altre ordinador ens dirà que la connexió ha sigut rebutjada.



Per obrir un servidor al primer ordinador és tan fàcil com executar la comanda:

sudo apt install openssh-server

I comprovar l’estat amb:

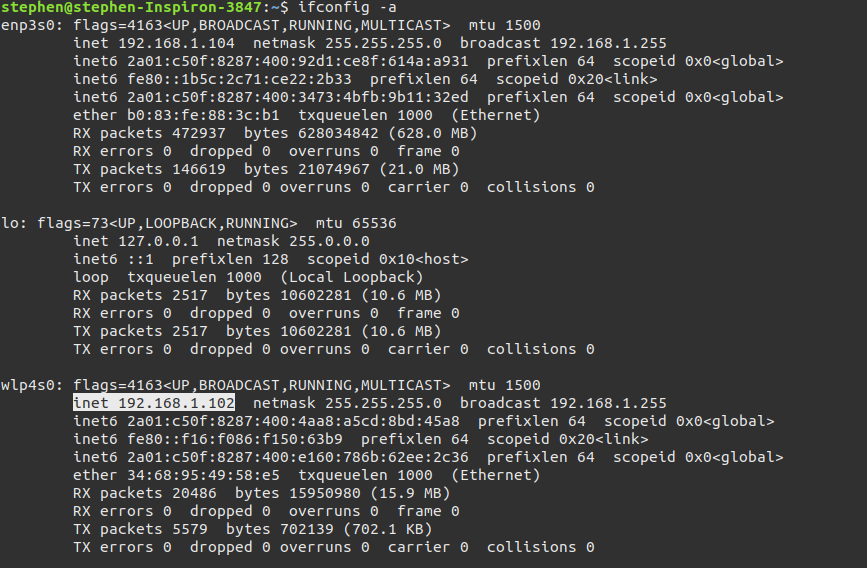
sudo systemctl status ssh

Ara si que podem intentar accedir al servidor amb ssh -X usuariHost@IP\_host.

Per fer-ho necessitem la ip del servidor que obtenim executant la comanda:

ifconfig -a

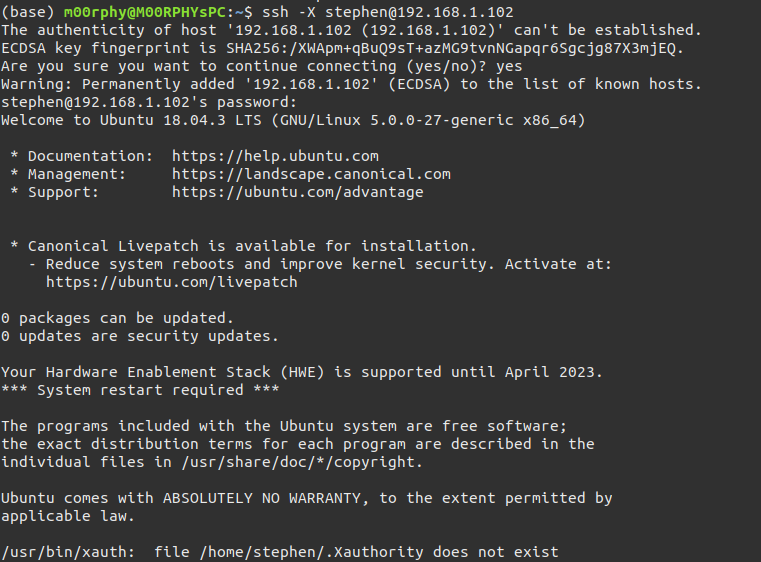
en el servidor on observem que la ip a la xarxa local és:



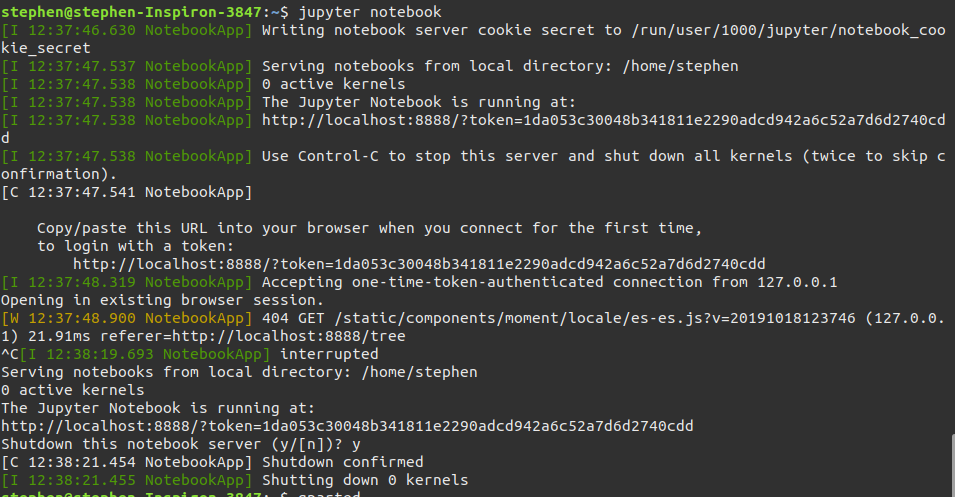
Al nostre cas al client hem executat:

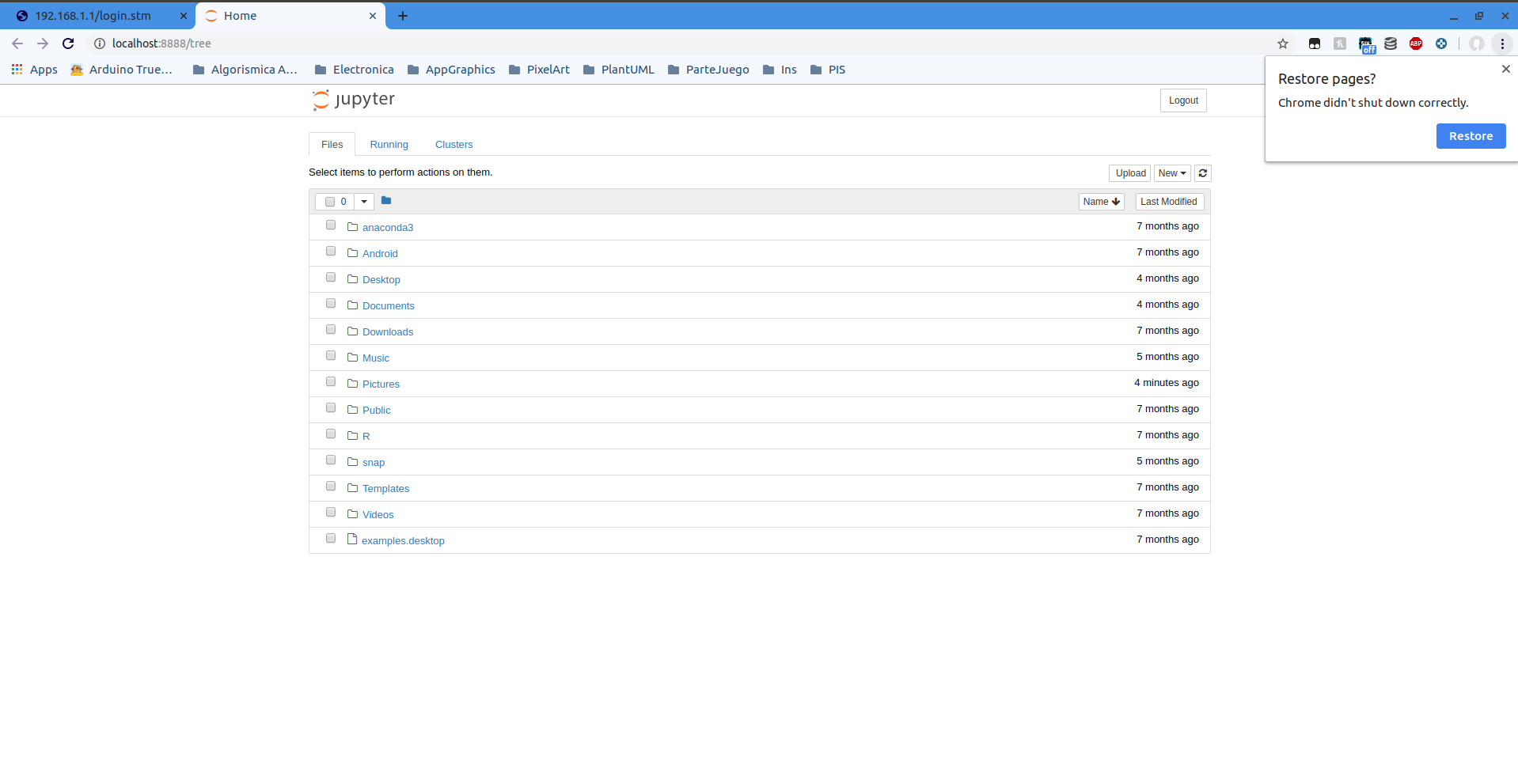
ssh -X stephen@192.168.1.102

i hem obtingut acces al servidor i executat algunes aplicacions del servidor des de el client com jupyter notebook.

****

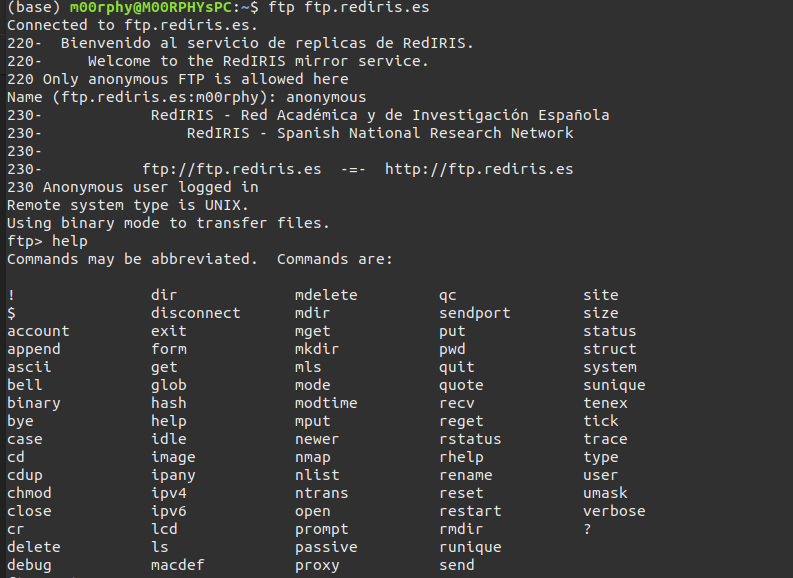
Al executar jupyter notebook des de el client, aquest es el que ha vist la execucio de la aplicació per terminal i ha sigut el servidor el que ha vist la obertura a una nova pestanya a Google Chrome amb el servidor de jupyter notebook.



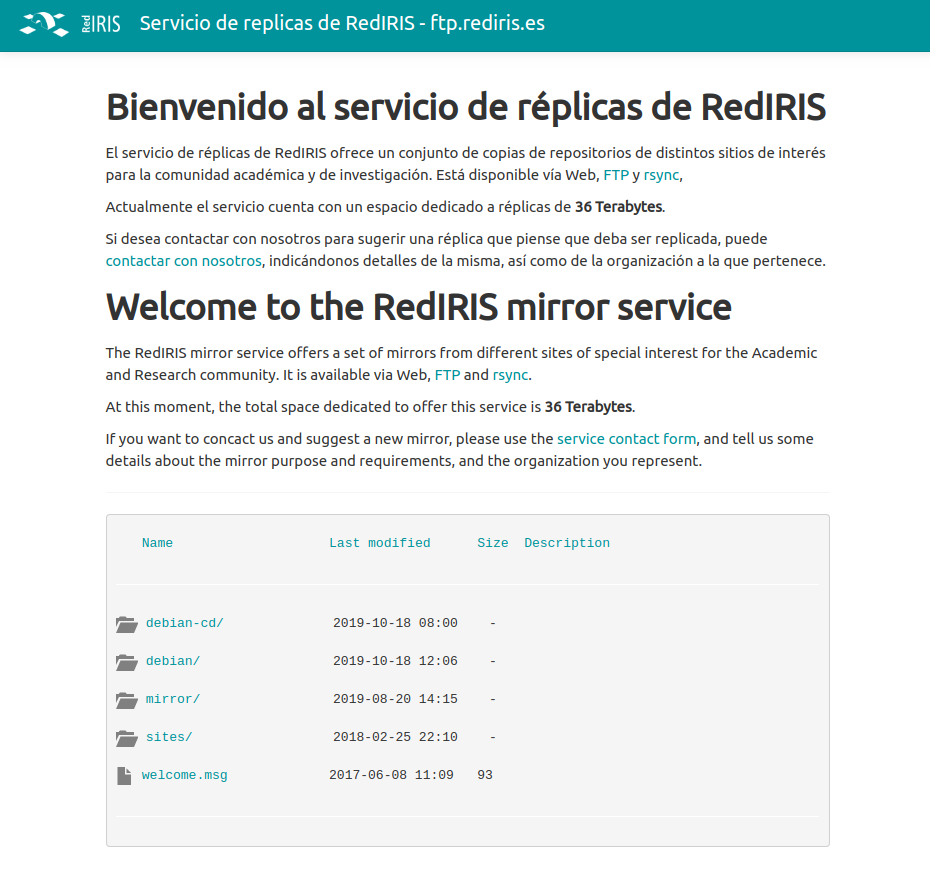


**FTP**

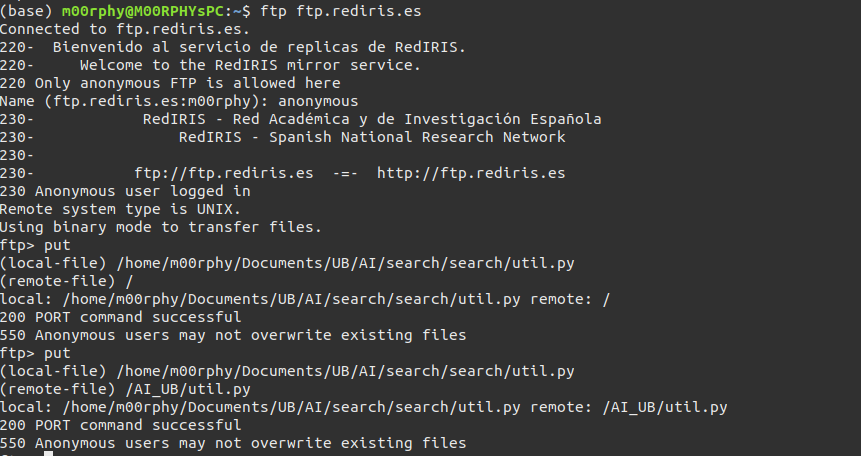
Hem provat ftp per poder entrar a la RedIRIS (“Red Académica y de Investigación Española”) com a usuari “anonymous” i provat les comandes suggerides.



No ens ha funcionat la comanda “ls” per poder veure el contingut del directori, pero hem anat a la un navegador i hem accedit des d’allà:

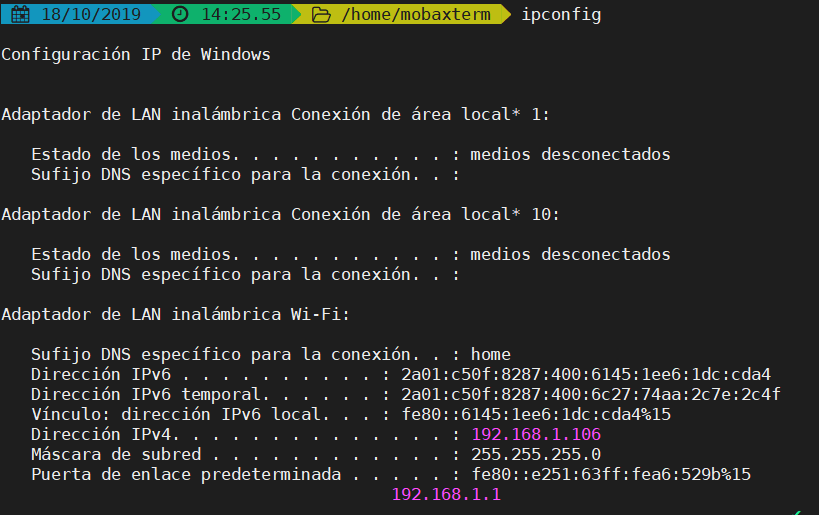


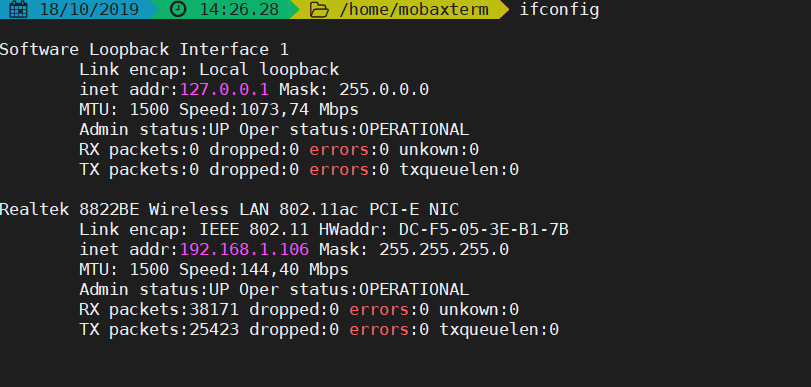
Hem vist que com a usuaris anònims no es pot pujar arxius, sino que és necessari accedir amb un usuari amb aquests permisos:



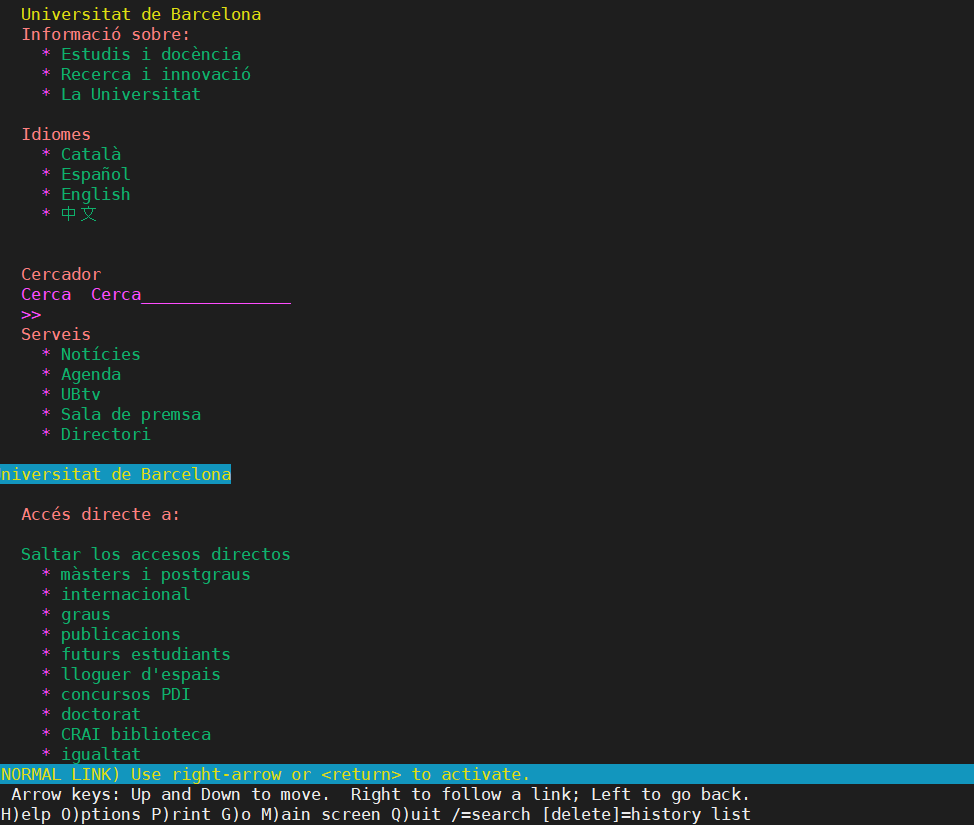
Seguidament hem instal·lat SW MobaXterm per a Windows 10 i hem provat el funcionament amb ifconfig i ipconfig, es un terminal que treballa tant amb les comandes que ja tenim a windows com amb les de linux.

Per tant la sortida de ipconfig es la que ja havíem vist anteriorment al terminal de windows, i ifconfig les que havíem vist a linux.





Hem instal·lat Lynx i ens hem donat compte de que és un “cercador d'ús general per la World Wide Web” que es pot ser útil per cercar a la web i accedir fàcilment en ocasions en les que no podem utilitzar un sistema operatiu amb interfície gràfica, com passa molts cops en servidors.



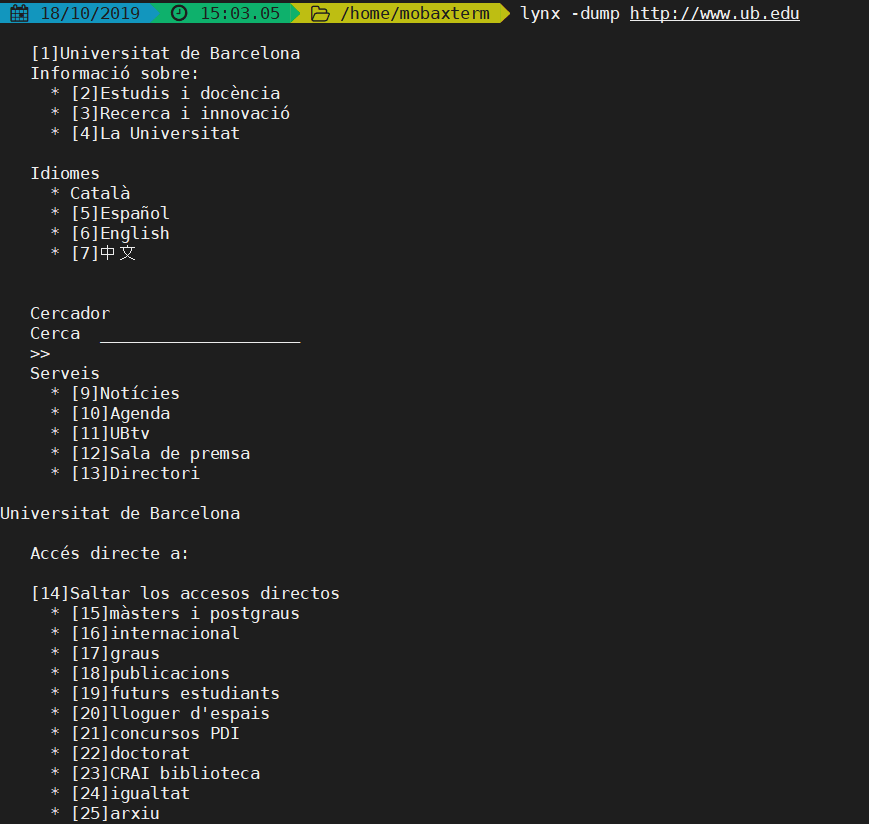
Si comparem el que hem obtingut amb el que ens mostraria per exemple el navegador Google Chrome, ens donem compte que és la mateixa informació, però amb lynx no ens mostra imatges o característiques gràfiques que té la web.



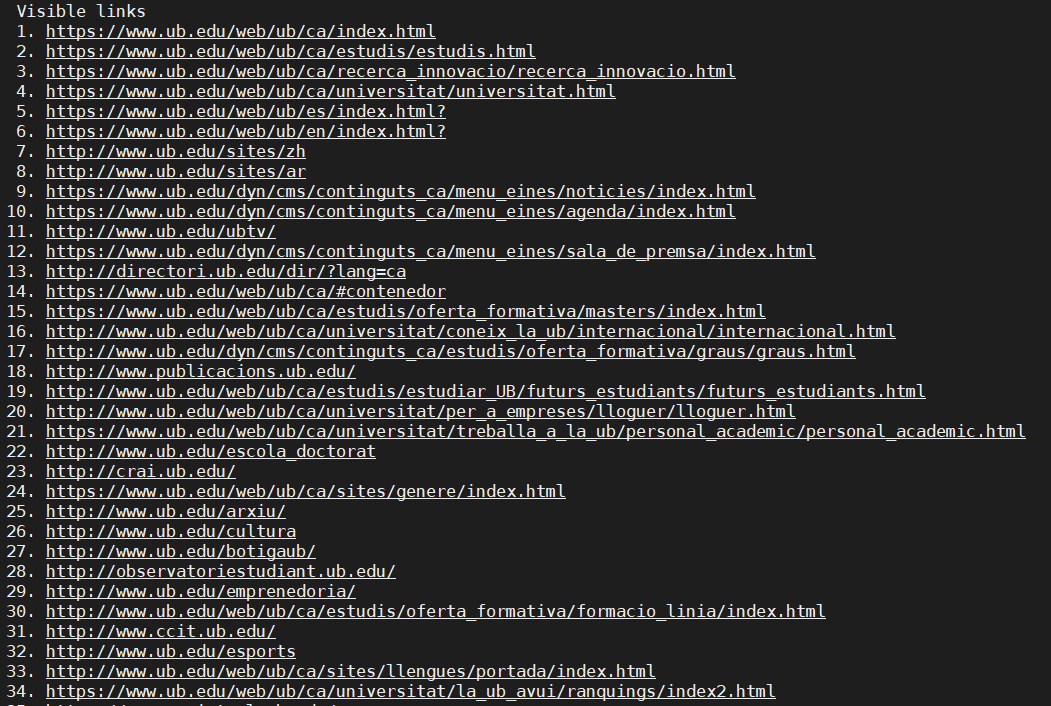
En executar:

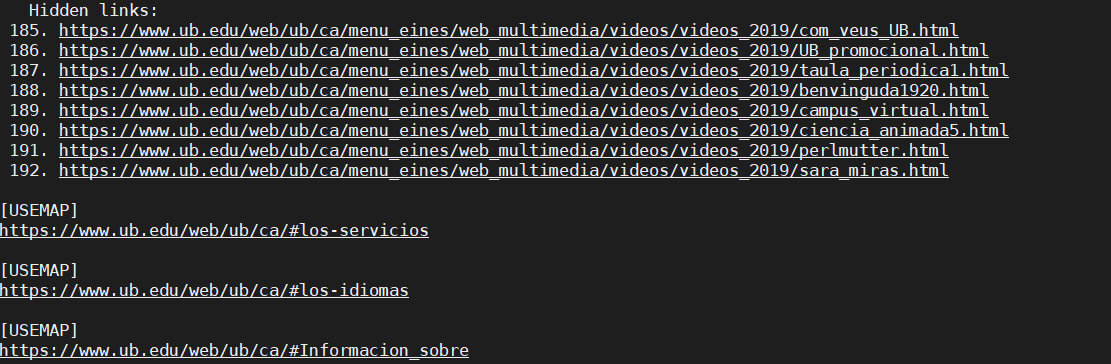
lynx -dump http://www.ub.edu

Hem vist que el que fa “-dump” es mostrar tota la informació que ens mostra la web, però ara en forma de text, i sense donar facilitats a l’hora de navegar, sinó que per navegar i moure’ns per aquesta pagina hauríem de fer-ho manualment executant “lynx -dump <link>” de nou sabent que aquest ens dona les possibles sortides d’aquesta pàgina. Es veu així:



Seguit de totes les direccions accessibles, visibles i no visibles que ens trobem a aquesta pàgina:





**FEINA REALITZADA AL LABORATORI**

En el primer dia de laboratori hem anat llegint la pràctica des del principi i hem anat provant les diferents comandes seguint les instruccions descrites en el pdf. En els moments que no enteníem alguna cosa, i no trobàvem la resposta en Internet, hem aprofitat que estàvem en classe per a preguntar al professor de pràctiques i profunditzar una mica més en algunes temes relacionades com per exemple en el ping i el TTL. En general, el primer dia hem anat provant les instruccions i ens hem anat familiaritzant amb elles, i hem entès els seus funcionaments. A més, hem anat responent les preguntes plantejades en la pràctica de forma oral. Com algunes comandes no funcionaven a l’aula com ara el telnet, les hem hagut de provar a casa.

En el segon dia, hem anat responent les preguntes ja en un document de text i hem anat profunditzant en cadascuna d’elles. Respondre aquestes preguntes d’una manera més tècnia i correcta ens ha ocupat les dues hores de laboratori, i hem preguntat al professor de laboratori alguns dubtes que teníem sobre el programa que havíem de fer.

**CONCLUSIONS**

Ens ha paregut una pràctica interessant per tal d’entendre els aspectes més bàsics relacionats amb les xarxes d’ordinadors. I ens ha servit per saber com funcionen algunes comandes i repassar alguns conceptes donades en teoria.

Pensem que hem assolit els objectius d’aquesta pràctica d’una manera satisfactòria ja que creiem que hem entès com funcionen les comandes que se’ns han proporcionat en aquesta pràctica i, a més, pensem que el programa que s’ha platejat funciona correctament.