



UNIVERSITAT^{DE}
BARCELONA

Pràctica 1: Introducció a les comunicacions

Antoni Tuduri
Alejandro Guzman

23 septembre 2022

ÍNDIX

1	Introducció	3
2	Objectius de la pràctica	3
3	Visualització de la xarxa	3
1	La IP	3
1.1	Com obtenim la IP? (Q1)	3
1.2	Protocol NAT	3
1.3	Tipus d'IPs (Q2)	6
4	Protocol intern del PC	6
1	Connexió amb màquina remota	7
1.1	Verificació de connexió amb nosaltres mateixos (Q3)	7
5	Verificació de connexió amb l'exterior	8
1	Verificació de connexió amb Google (Q4)	8
2	Ruta dels datagrames enviats (Q5)	8
6	Coneixement de l'entorn proper	9
1	La MAC o adreça física (Q6)	10
7	Estadístiques de xarxa (Q8)	11
8	Connexions amb servidors	13
1	Telnet (Q9 i Q10)	13
2	ssh (Q11 i Q12)	13
3	FTP (Q13)	14
4	LYNX (Q13)	15
9	Sockets i Aplicació Pràctica	16
10	Conclusions	18

1 INTRODUCCIÓ

En aquesta pràctica durem a terme connexions entre ordinadors diferents per via de comandaments de consola. Aquestes comandes són iguals o molt semblants entre Linux, MAC i Windows (nosaltres fem servir aquest últim). Així entendrem com funcionen els diferents programes que ho fan de manera interna.

Tambe veurem que hi ha diferents tipus de direccions IP, i el com diferenciar-les.

Finalment aprendrem a com connectar-nos a diferents servidors mitjançant diverses eines com SSH o Telnet i finalitzarem amb la creació d'un xat entre dos dispositius de forma remota.

2 OBJECTIUS DE LA PRÀCTICA

Els principals objectius de la primera pràctica de l'assignatura són:

- L'ús de comandaments per comunicació amb la xarxa
- Aprendre a com podem obtenir informació i estadístiques de la xarxa.
- Connectar-nos a diversos servidors gràcies al coneixement de les seves IPs i de comandaments específiques.
- Crear un xat servidor-client per múltiples usuaris

A part aquesta pràctica ens servirà per endinsar-nos en el món de les xarxes i aplicar els conceptes teòrics explicats a classe per aplicar els seus diversos usos a aplicacions pràctiques.

3 VISUALITZACIÓ DE LA XARXA

1 La IP

L'adreça IP privada és una adreça fixa que s'assigna a cada dispositiu connectat a una xarxa privada o domèstica, és a dir, l'adreça IP que el router assigna a cada ordinador, smartphones, smart TV, tablet, consola de joc o qualsevol altre dispositiu connectat a ell. Així, cada dispositiu connectat a un router té la seva pròpia adreça IP privada, mentre comparteixen la mateixa IP pública. Les adreces IP privades no són accessibles des d'Internet i no canvien, llevat que les assignem nosaltres manualment.

1.1 Com obtenim la IP? (Q1)

La obtenció de la IP en el nostre ordinador es realitza accedint a la terminal de Windows i introduir la comanda `ipconfig/all`, l'execució de la qual genera la següent sortida:

Un cop hem visualitzat la considerable quantitat de dades que ens proporciona l'output d'aquesta comanda, obtenim la IP buscant en aquest cas on es menciona IPv4.

1.2 Protocol NAT

Internet no va ser concebut inicialment com una xarxa tan gran com el que és ara, per la qual cosa únicament es van assignar 32 bits per a les adreces IP, la qual cosa permetia crear 4294967296 adreces IP diferents.

L'augment de la popularitat d'Internet va fer que cada vegada hi hagués més dispositius connectats a ell, fet que va provocar que s'acabessin les adreces IP. Aquest problema va obligar a

```

C:\Users\darby>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : LAPTOP-SRFEBUF8
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: home

Adaptador de Ethernet Ethernet 6:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-0A
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::cca4:7115:12f2:8914%10(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 805961767
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-E7-08-88-74-D8-3E-06-05-59
NetBIOS sobre TCP/IP. . . . . : habilitado

```

Figura 3.1: Output de la comanda ipconfig/all part 1

```

Adaptador de LAN inalámbrica Conexión de área local* 3:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Dirección física. . . . . : 74-D8-3E-06-05-5A
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 4:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Dirección física. . . . . : 76-D8-3E-06-05-59
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

```

Figura 3.2: Output de la comanda ipconfig/all part 2

crear algun tipus de mecanisme per a reduir el número d'IP's existents. Aquest mecanisme és el protocol NAT.

El protocol NAT és un mecanisme que tradueix IP's privades a IP's públiques i viceversa. La idea és que cada node d'una xarxa privada posseeixi una IP privada per a comunicar-se amb els altres nodes d'aquesta xarxa, mentre que per a accedir a Internet utilitzarà una adreça IP pública. Això redueix enormement el número d'IP's que hi ha circulant en Internet.

A la NAT hi ha diversos tipus de funcionament:

- Estatica: Una adreça IP privada es tradueix sempre en una mateixa adreça IP publica. Aquesta manera de funcionament permetria a un host dins de la xarxa ser visible des d'Internet.
- Dinamica: El router te assignades diverses adreces IP publiques, de manera que cada adreça IP privada es mapeja usant una de les adreces IP publiques que el router te assignades, de manera que a cada adreça IP privada li correspon almenys una adreça IP pub-

```

Adaptador de LAN inalámbrica Wi-Fi:

  Sufijo DNS específico para la conexión. . . : home
  Descripción . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
  Dirección física. . . . . : 74-D8-3E-06-05-59
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::f053:478e:d6ee:dcbb%6(Preferido)
  Dirección IPv4. . . . . : 192.168.1.17(Preferido)
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : martes, 18 de octubre de 2022 19:18:39
  La concesión expira . . . . . : jueves, 20 de octubre de 2022 9:28:27
  Puerta de enlace predeterminada . . . . : 192.168.1.1
  Servidor DHCP . . . . . : 192.168.1.1
  IAID DHCPv6 . . . . . : 74766398
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-E7-08-88-74-D8-3E-06-05-59
  Servidores DNS. . . . . : 192.168.1.1
  NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:

  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Bluetooth Device (Personal Area Network)
  Dirección física. . . . . : 74-D8-3E-06-05-5D
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí

```

Figura 3.3: Output de la comanda ipconfig/all part 3

```

Adaptador de LAN inalámbrica Wi-Fi:

  Sufijo DNS específico para la conexión. . . : home
  Descripción . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
  Dirección física. . . . . : 74-D8-3E-06-05-59
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::f053:478e:d6ee:dcbb%6(Preferido)
  Dirección IPv4. . . . . : 192.168.1.17(Preferido)
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : martes, 18 de octubre de 2022 19:18:39
  La concesión expira . . . . . : jueves, 20 de octubre de 2022 9:28:27
  Puerta de enlace predeterminada . . . . : 192.168.1.1
  Servidor DHCP . . . . . : 192.168.1.1
  IAID DHCPv6 . . . . . : 74766398
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-E7-08-88-74-D8-3E-06-05-59
  Servidores DNS. . . . . : 192.168.1.1
  NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:

  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Bluetooth Device (Personal Area Network)
  Dirección física. . . . . : 74-D8-3E-06-05-5D
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí

```

Figura 3.4: Output de la comanda ipconfig/all part 3

lica.

Cada vegada que un host requereixi una connexio a Internet, el router li assignara una adreça IP publica que no estigui sent utilitzada. En aquesta ocasio s'augmenta la seguretat ja que dificulta que un host extern ingressi a la xarxa ja que les adreces IP publiques van canviant.

- Sobrecarrega: La NAT amb sobrecarrega o PAT (Port Address Translation) es el mes comu de tots els tipus, ja que es l'utilitzat a les llars. Es poden mapejar multiples adreces IP privades a traves d'una adreça IP publica, de manera que evitem contractar mes d'una

adreça IP pública. A més de l'estalvi econòmic, també s'estalvien adreces IPv4, ja que encara que la subxarxa nombroses màquines, totes surten a Internet a través d'una mateixa adreça IP pública.

Per poder fer això el router fa ús dels ports. En els protocols TCP i UDP es disposen de 65.536 ports per establir connexions. De manera que quan una màquina vol establir una connexió, el router guarda la seva IP privada i el port d'origen i els associa a la IP pública i un port a l'atzar. Quan arriba informació a aquest port triat a l'atzar, el router comprova la taula i el reenvia a la IP privada i port que corresponguin.

1.3 Tipus d'IPs (Q2)

Si es classifiquen les adreces IP en funció de la seva persistència, únicament poden existir els següents tipus:

- No volàtil o estàtica: Són aquelles que s'assignen de forma permanent a un dispositiu o router.
- Volàtil o dinàmica: Són aquelles que s'assignen cada vegada que el dispositiu o router es connecta a Internet.

Per tal d'esbrinar si la nostra IP canvia cada vegada que ens connectem a Internet, provarem de desconnectar-nos i connectar-nos a Internet diverses vegades. Aquesta tasca la portarem a terme mitjançant les següents comandes:

- `ipconfig/release`: Serveix per a alliberar la nostra IP, el que es podria traduir com a desconnectar-nos d'Internet.
- `ipconfig/renew`: Serveix per a demanar una IP, el que es podria traduir com a connectar-nos a Internet.

El mètode consisteix en executar aquestes dues comandes (primer `ipconfig/release` i després `ipconfig/renew`) diverses vegades per tal de comprovar si aquesta canvia i és dinàmica o en canvi és invariable i per tant és estàtica.

Després d'uns pocs intents, la nostra IP segueix sent la mateixa. Uns intents més hem observat que en una de les execucions de `ipconfig/renew` la nostra IP ha passat a ser 192.168.1.35, per tant, podem afirmar que la nostra IP és dinàmica.

4 PROTOCOL INTERN DEL PC

Un cop coneixem què és exactament una IP, com tractar-la i mecanismes de traducció en la xarxa, verifiquem si realment aquesta IP és visible a la xarxa.

Per tal d'arribar a aquest objectiu ens ajudarem de la comanda `ping`, que s'utilitza per a diagnosticar possibles errors de xarxa entre un host local amb una altra màquina remota, tots dos connectats.

La comanda `ping` s'utilitza per a enviar a una màquina remota un missatge amb una sol·licitud d'eco, i es vol que es contesti amb una resposta d'eco per a poder verificar que el missatge que li hem enviat ha arribat en una xarxa de tipus TCP/IP. Per tant si falla vol dir que hi ha un error en la nostra targeta de connexió a la xarxa local (NIC).

1 Connexió amb màquina remota

La primera part d'aquest exercici es realitzar una connexió amb una màquina remota tal i com ens sol·licita l'enunciat. Per això utilitzarem la comanda ping 161.116.95.254, amb la qual verificarem l'estat de la nostra connexió amb la màquina remota.

```
C:\Users\darby>ping 161.116.95.254

Haciendo ping a 161.116.95.254 con 32 bytes de datos:
Respuesta desde 161.116.95.254: bytes=32 tiempo=3ms TTL=250
Respuesta desde 161.116.95.254: bytes=32 tiempo=3ms TTL=250
Respuesta desde 161.116.95.254: bytes=32 tiempo=7ms TTL=250
Respuesta desde 161.116.95.254: bytes=32 tiempo=2ms TTL=250

Estadísticas de ping para 161.116.95.254:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 7ms, Media = 3ms
```

Figura 4.1: Output de la comanda ping 161.116.95.254 amb internet

Com es pot veure s'han enviat quatre paquets i la màquina remota ens ha retornat feedback dels quatre i cap s'ha perdut, per tant podem afirmar que ens podem comunicar amb la màquina correctament.

En canvi si desactivem l'internet i tornem a executar la comanda observem el següent:

```
C:\Users\darby>ping 161.116.95.254

Haciendo ping a 161.116.95.254 con 32 bytes de datos:
Error general.
Error general.
Error general.
Error general.

Estadísticas de ping para 161.116.95.254:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Figura 4.2: Output de la comanda ping 161.116.95.254 sense internet

Com podem comprovar cap paquet s'ha pogut enviar, conseqüència directa de tenir internet al nostre dispositiu, que impossibilita la possibilitat de comunicar-se amb l'exterior.

1.1 Verificació de connexió amb nosaltres mateixos (Q3)

Hem comprovat la connexió amb una màquina remota, ara comprovarem la mateixa comanda però amb la IP 127.0.0.1 amb el següent resultat:

```
C:\Users\darby>ping 161.116.95.254

Haciendo ping a 161.116.95.254 con 32 bytes de datos:
Error general.
Error general.
Error general.
Error general.

Estadísticas de ping para 161.116.95.254:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
      (100% perdidos),
```

Figura 4.3: Output de la comanda ping 127.0.0.1 amb internet

Com s'ha mencionat anteriorment, la comanda ping serveix com a diagnòstic de problemes de xarxa enviant paquets a una adreça IP que s'especifica a continuació. Sabent això només cal afegir que l'adreça IP 127.0.0.1 és la coneguda com a adreça de loopback, ja que fa referència a la mateixa màquina des de la qual executem la comanda.

D'aquesta forma la comanda ping 127.0.0.1 envia paquets a la mateixa màquina, per tant inclús funciona sense internet perquè no es necessita de cap màquina remota ni connexió externa per comunicar-nos amb nosaltres mateixos.

5 VERIFICACIÓ DE CONNEXIÓ AMB L'EXTERIOR

Havent verificat el correcte funcionament del protocol intern del PC, ens queda comprovar el correcte funcionament de la connexió amb l'exterior.

1 Verificació de connexió amb Google (Q4)

Primerament comprovarem la nostra connexió amb els servidors de Google, així que utilitzarem la comanda ping un altre cop, ara introduïnt la direcció web de Google, enviant les sol·licituds d'ECO a aquesta pàgina i a l'espera de rebre una resposta ECO per part seva.

Executem la comanda ping www.google.com a la consola tal i com hem fet anteriorment: Com es pot observar i assegurar, la connexió amb www.google.com és efectiva des de la nostra màquina degut a que hem rebut resposta de tots els paquets enviats.

A les darreres línies observem que el temps aproximat d'anada i tornada per a cada paquet oscil·la entre 14 i 20 mil·lisegons amb una mitjana de 16 mil·lisegons.

2 Ruta dels datagrames enviats (Q5)

Un cop hem verificat el correcte funcionament de la comunicació entre la nostra màquina i www.google.com, obtenim la ruta completa que ha seguit el datagrama que s'ha enviat a google amb la comanda ping www.google.com.


```
C:\Users\darby>ping www.google.com

Haciendo ping a www.google.com [142.250.185.4] con 32 bytes de datos:
Respuesta desde 142.250.185.4: bytes=32 tiempo=14ms TTL=115
Respuesta desde 142.250.185.4: bytes=32 tiempo=16ms TTL=115
Respuesta desde 142.250.185.4: bytes=32 tiempo=20ms TTL=115
Respuesta desde 142.250.185.4: bytes=32 tiempo=16ms TTL=115

Estadísticas de ping para 142.250.185.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 20ms, Media = 16ms
```

Figura 5.1: Output de la comanda ping www.google.com

La ruta que volem obtenir està composta per totes les adreces IP per les quals ha passat el datagrama abans d'arribar a l'adreça IP de Google.

En windows executem la comanda tracert www.google.com per obtenir la ruta mencionada:

```
C:\Users\darby>tracert www.google.com

Traza a la dirección www.google.com [142.250.184.164]
sobre un máximo de 30 saltos:

  1    14 ms    11 ms    10 ms  10.133.255.254
  2     2 ms     2 ms     3 ms  10.199.12.3
  3     3 ms     5 ms     6 ms  10.199.20.2
  4     4 ms     7 ms     3 ms  anella-ub2.cesca.cat [84.88.18.113]
  5    11 ms    11 ms    14 ms  google.02.catnix.net [193.242.98.156]
  6    12 ms    12 ms    12 ms  74.125.242.161
  7    13 ms    11 ms    11 ms  142.250.213.125
  8    11 ms    12 ms    11 ms  mad07s23-in-f4.1e100.net [142.250.184.164]

Traza completa.
```

Figura 5.2: Output de la comanda tracert www.google.com

La ruta que segueix el datagrama és la que es pot veure en l'output en forma descendent en la darrera columna. Totes les adreces IP són públiques, a excepció de la primera que correspon a la nostra IP privada.

En aquest cas no apareix el símbol "*" en cap lloc, aquest símbol apareix en una fila sencera indicant una adreça concreta del recorregut, llavors el paquet que venia de la adreça anterior a "*" no ha pogut connectar-se a la IP que volia durant el temps reservat per a establir la connexió, per tant passa a una altra IP (la següent al símbol en la taula).

6 CONEIXEMENT DE L'ENTORN PROPER

El nostre ordinador es connecta a la xarxa amb cable Ethernet o WIFI mitjançant el protocol 802.x amb el qual la xarxa exigeix que s'especifiquin les MAC de les màquines origen i destí de la connexió.

1 La MAC o adreça física (Q6)

L'adreça MAC és un identificador únic que cada fabricant assigna a la targeta de xarxa dels dispositius connectats, des d'un ordinador o mòbil fins a routers, impressores o altres dispositius. Les sigles vénen de l'anglès, i signifiquen Media Access Control. Com que hi ha dispositius amb diferents targetes de xarxa, com una per a WiFi i una altra per a Ethernet, alguns poden tenir diferents adreces MAC depenent de per on es connectin.

Amb la comanda `ipconfig/all` podem veure diversos apartats, en l'apartat de connexió wifi trobem la configuració de la connexió a la xarxa local WI-FI, podem trobar la direcció física (o adreça mac), aquesta és 74-D8-3E-06-05-59, està escrita en hexadecimal i té un total de 48 bits, totes les adreces mac tenen la mateixa mida.

Per obtenir les adreces IP i MAC de la màquina destí amb la qual volem establir connexió tenim el protocol ARP (Address Resolution Protocol). Aquest protocol envia des del PC origen un paquet donant la informació de les adreces IP i MAC origen i l'adreça IP destí, i demana com a resposta l'adreça MAC destí. Si el dispositiu al qual volem accedir està dins la mateixa xarxa, serà aquest mateix qui enviarà un ARP Response proporcionant l'adreça MAC.

En cas contrari, si no es troben els dos dispositius a la mateixa xarxa, qui contestarà al ARP Request serà el router de sortida.

La comanda `arp` té diferents opcions. Una d'elles és `arp -a`, que ens mostra la taula dinàmica:

```
C:\Windows\System32>arp -a

Interfaz: 10.133.25.193 --- 0x6
  Dirección de Internet      Dirección física      Tipo
  10.133.255.254             00-08-e3-ff-fc-50     dinámico
  10.133.255.255             ff-ff-ff-ff-ff-ff     estático
  224.0.0.2                  01-00-5e-00-00-02     estático
  224.0.0.22                 01-00-5e-00-00-16     estático
  224.0.0.251                01-00-5e-00-00-fb     estático
  224.0.0.252                01-00-5e-00-00-fc     estático
  239.255.255.250            01-00-5e-7f-ff-fa     estático
  255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.56.1 --- 0xa
  Dirección de Internet      Dirección física      Tipo
  192.168.56.255             ff-ff-ff-ff-ff-ff     estático
  224.0.0.22                 01-00-5e-00-00-16     estático
  224.0.0.251                01-00-5e-00-00-fb     estático
  224.0.0.252                01-00-5e-00-00-fc     estático
  239.255.255.250            01-00-5e-7f-ff-fa     estático
```

Figura 6.1: Output de la comanda `arp -a`

(Q7) La taula dinàmica té 13 entrades. Ara esborrarem una entrada dinàmica amb la comanda `arp -d 10.133.255.254` on la IP és pròpia de la entrada que volem esborrar, llavors l'output de-

sprés de d'esborrarla de la comanda arp -a és la mateixa taula però observem que ja no es troba la entrada dinàmica esborrada:

```
C:\Windows\System32>arp -d 10.133.255.254

C:\Windows\System32>arp -a

Interfaz: 10.133.25.193 --- 0x6
  Dirección de Internet      Dirección física      Tipo
  10.133.255.254            00-08-e3-ff-fc-50    dinámico
  10.133.255.255            ff-ff-ff-ff-ff-ff    estático
  224.0.0.2                  01-00-5e-00-00-02    estático
  224.0.0.22                 01-00-5e-00-00-16    estático
  224.0.0.251                01-00-5e-00-00-fb    estático
  224.0.0.252                01-00-5e-00-00-fc    estático
  239.255.255.250            01-00-5e-7f-ff-fa    estático
  255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0xa
  Dirección de Internet      Dirección física      Tipo
  192.168.56.255            ff-ff-ff-ff-ff-ff    estático
  224.0.0.22                 01-00-5e-00-00-16    estático
  224.0.0.251                01-00-5e-00-00-fb    estático
  224.0.0.252                01-00-5e-00-00-fc    estático
  239.255.255.250            01-00-5e-7f-ff-fa    estático
```

Figura 6.2: Output de la comanda arp -a després d'esborrar una entrada dinàmica

7 ESTADÍSTIQUES DE XARXA (Q8)

Netstat és una eina que ens detalla informació sobre les connexions actives del nostre ordinador.

La comanda netstat -h ens mostra totes les comandes disponibles d'aquesta eina. En concret, se'ns demana executar la comanda netstat -r, que mostra el contingut de la taula de Routing:

```
C:\Users\darby>netstat -r

=====
Ilista de interfaces
 10...0a 00 27 00 00 0a .....VirtualBox Host-Only Ethernet Adapter
  3...74 d8 3e 06 05 5a .....Microsoft Wi-Fi Direct Virtual Adapter #3
 24...76 d8 3e 06 05 59 .....Microsoft Wi-Fi Direct Virtual Adapter #4
  6...74 d8 3e 06 05 59 .....Intel(R) Wi-Fi 6 AX200 160MHz
 14...74 d8 3e 06 05 5d .....Bluetooth Device (Personal Area Network)
  1.....Software Loopback Interface 1
=====
```

Figura 7.1: Output de la comanda netstat -r primera part

```

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.1.1           192.168.1.17  50
127.0.0.0           255.0.0.0           En vínculo             127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo             127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo             127.0.0.1     331
192.168.1.0         255.255.255.0       En vínculo             192.168.1.17  306
192.168.1.17        255.255.255.255     En vínculo             192.168.1.17  306
192.168.1.255       255.255.255.255     En vínculo             192.168.1.17  306
192.168.56.0        255.255.255.0       En vínculo             192.168.56.1  281
192.168.56.1        255.255.255.255     En vínculo             192.168.56.1  281
192.168.56.255      255.255.255.255     En vínculo             192.168.56.1  281
224.0.0.0           240.0.0.0           En vínculo             127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo             192.168.56.1  281
224.0.0.0           240.0.0.0           En vínculo             192.168.1.17  311
255.255.255.255     255.255.255.255     En vínculo             127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo             192.168.56.1  281
255.255.255.255     255.255.255.255     En vínculo             192.168.1.17  311
=====
Rutas persistentes:
Ninguno

```

Figura 7.2: Output de la comanda netstat -r segona part

```

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
1 331 ::1/128                       En vínculo
10 281 fe80::/64                     En vínculo
6 311 fe80::/64                     En vínculo
10 281 fe80::cca4:7115:12f2:8914/128 En vínculo
6 311 fe80::f053:478e:d6ee:dcbb/128 En vínculo
1 331 ff00::/8                      En vínculo
10 281 ff00::/8                      En vínculo
6 311 ff00::/8                      En vínculo
=====
Rutas persistentes:
Ninguno

```

Figura 7.3: Output de la comanda netstat -r tercera part

La opció -r mostra la taula d'enrutament, aquesta taula llista conté tota la informació necessària per a que un paquet de dades pugui viatjar fins arribar al destí de forma òptima com l'origen i el destí. També apareixen les mètriques. Una mètrica és un valor assignat a una ruta IP per a una interfície de xarxa determinada. Identifica el cost associat a aquesta ruta. Per exemple, la mètrica es pot valorar en termes de velocitat d'enllaç, recompte de salts o retard de temps.

En executar la comanda netstat -a es mostren totes les connexions i ports que s'estàn fent servir en aquell moment, a part és una llista que s'actualitza a mesura que noves connexions es van establint.

Conexiones activas			
Proto	Dirección local	Dirección remota	Estado
TCP	0.0.0.0:135	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:1042	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:1043	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:1337	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:5357	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:5426	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:6000	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:7680	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:9012	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:9013	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:12177	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49667	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49671	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:49674	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:53688	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:53689	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:54235	LAPTOP-SRFEBUF8:0	LISTENING
TCP	0.0.0.0:54236	LAPTOP-SRFEBUF8:0	LISTENING
TCP	127.0.0.1:1043	LAPTOP-SRFEBUF8:50831	ESTABLISHED
TCP	127.0.0.1:3213	LAPTOP-SRFEBUF8:0	LISTENING
TCP	127.0.0.1:6000	LAPTOP-SRFEBUF8:56680	ESTABLISHED
TCP	127.0.0.1:6000	LAPTOP-SRFEBUF8:56681	ESTABLISHED

Figura 7.4: Output de la comanda netstat -a

8 CONNEXIONS AMB SERVIDORS

En aquest apartat se'ns presenten tres comandes bàsiques per connectar-nos amb servidors.

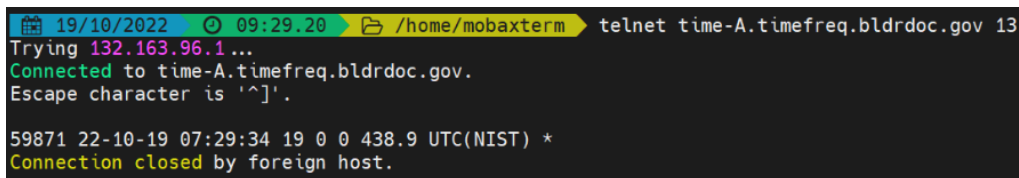
- Telnet: És un protocol de xarxa TCP/IP que s'utilitza per establir connexions remotes amb una altra màquina.
- ftp: És un protocol per la transferència d'arxius entre sistemes connectats a una xarxa, basada en l'arquitectura client - servidor.
- ssh: És un protocol que permet una connexió remota segura entre dues màquines. És més segura que Telnet perquè aquesta encripta la connexió.

1 Telnet (Q9 i Q10)

Primerament ens connectem a time-A.timefreq.bldrdoc.gov 13 i ens retorna la data completa en la qual ens hem connectat.

2 ssh (Q11 i Q12)

Una altra forma de poder connectar-se amb una màquina de forma remota és fent servir ssh, es pot fer servir en diversos sistemes operatius, se'ns recomana fer servir Linux o, en cas que tinguem Windows al nostre dispositiu (com és el nostre cas), ens descarreguem l'aplicació MobaXtrem, la qual és bàsicament un terminal millorat per a Windows amb servidor X11, client



```

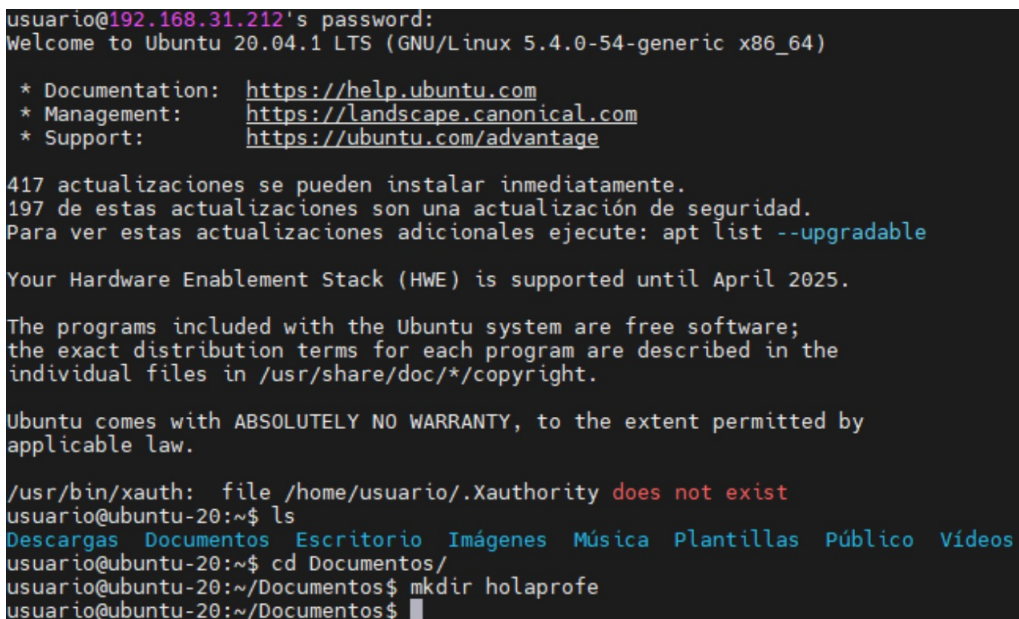
19/10/2022 09:29.20 /home/mobaxterm telnet time-A.timefreq.bldrdoc.gov 13
Trying 132.163.96.1...
Connected to time-A.timefreq.bldrdoc.gov.
Escape character is '^]'.
59871 22-10-19 07:29:34 19 0 0 438.9 UTC(NIST) *
Connection closed by foreign host.

```

Figura 8.1: Output de la comanda time-A.timefreq.bldrdoc.gov 13

SSH amb pestanyes, network tools i més prestacions.

Si executem la comanda `ssh -X usuario@192.168.31.212` (essent usuari el hostname i 192.168.31.212 la host IP) i introduïm la contrasenya del dispositiu al qual ens volem connectar, tindrem accés a la CLI (command line interface) del segon dispositiu remotament.



```

usuario@192.168.31.212's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

417 actualizaciones se pueden instalar inmediatamente.
197 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

/usr/bin/xauth: file /home/usuario/.Xauthority does not exist
usuario@ubuntu-20:~$ ls
Descargas Documentos Escritorio Imágenes Música Plantillas Público Vídeos
usuario@ubuntu-20:~$ cd Documentos/
usuario@ubuntu-20:~/Documentos$ mkdir holaprofe
usuario@ubuntu-20:~/Documentos$

```

Figura 8.2: Connexió remota a un segon dispositiu

I des de el segon dispositiu al qual ens hem connectat remotament comprovem que efectivament el contingut és el mateix.



```

root@ubuntu-20:/home# ls
usuario
root@ubuntu-20:/home# cd usuario/
root@ubuntu-20:/home/usuario# ls
Descargas Documentos Escritorio Imágenes Música Plantillas Público Vídeos
root@ubuntu-20:/home/usuario# cd Documentos/
root@ubuntu-20:/home/usuario/Documentos# ls
holaprofe

```

Figura 8.3: Vista des del segon dispositiu

3 FTP (Q13)

Si executem la comanda `man ftp` des de un terminal de linux podem veure el manual de la comanda ftp i els diferents arguments d'execució que es poden utilitzar. Si executem la comanda

```
18/10/2022 23:00.40 /home/mobaxterm ftp ftp.rediris.es
Connected to ftp.rediris.es.
220- Bienvenido al servicio de replicas de RedIRIS.
220- Welcome to the RedIRIS mirror service.
220 Only anonymous FTP is allowed here
```

Figura 8.4: Connexió remota a un segon dispositiu

ftp ftp.rediris.es ens connectem al "servicio de replicas de RedIRIS".

```
18/10/2022 23:00.40 /home/mobaxterm ftp ftp.rediris.es
Connected to ftp.rediris.es.
220- Bienvenido al servicio de replicas de RedIRIS.
220- Welcome to the RedIRIS mirror service.
220 Only anonymous FTP is allowed here
```

Figura 8.5: Output de la comanda ftp ftp.rediris.es

Podem provar de descarregar un fitxer qualsevol com per exemple el welcome.msg que conté el missatge de benvolguda. Ho fem utilitzant mget.

```
ftp> mget welcome.msg
mget welcome.msg? y
200 PORT command successful
150 Connecting to port 57128
226-File successfully transferred
226 0.000 seconds (measured here), 428.01 Kbytes per second
93 bytes received in 0.000316 seconds (294303 bytes/s)
```

Figura 8.6: Output de la comanda mget welcome.msg

Si anem a la nostra carpeta arrel, podem comprovar que s'ha descarregat l'arxiu i que conté el missatge de benvolguda.

També podem intentar pujar un fitxer amb la comanda put, però els usuaris anònims no tenen permís per fer-ho, per tant no ens deixa.

4 LYNX (Q13)

Respecte a les diferències entre ipconfig i ifconfig, ipconfig mostra totes les interfícies de xarxes sense importar si estan actives o no i ifconfig només les que estan habilitades.

Si executem la comanda lynx <http://www.ub.edu>, podem veure com se'ns mostra la web de la UB en format de text i se'ns permet navegar per ella. Amb la comanda lynx <http://www.ub.edu> -dump se'ns mostra la web amb el text que conté i se'ns mostren tots els enllaços a altres direccions web que apareixen. Aquesta comanda pot tenir diverses utilitats, ja que ens podria permetre fer programes que utilitzin aquestes comandes per cercar paraules clau en diferents webs, fer estadístiques sobre quins són els hyperlinks més freqüents, etc.

```

IFRAME: https://www.googletagmanager.com/ns.html?id=GTM-MLPG24R

Skip to main content

CA
CA ES EN

Universitat de Barcelona

Universitat de Barcelona

*
*
*
*
*
*
*

* Aprèn
* Investiga
* Col·labora
* La UB

* Aprèn
* Investiga
* Col·labora
* La UB

```

Figura 8.7: Output de la comanda lynx `http://www.ub.edu`

9 SOCKETS I APLICACIÓ PRÀCTICA

Aquest projecte està conformat per dues parts; el servidor (constantment en execució, rep cada missatge i ho notifica) i el client (es connecta al servidor i envia i rep missatges de la resta de clients).

A continuació mostrem el codi realitzat gràcies a l'ajuda del tutorial de Python proporcionat en l'enunciat de la pràctica:

```

# CLIENT
import socket
from threading import Thread

def admit():
    while True:
        missatge = admit_from_socket ()
        print (missatge)

def admit_from_socket():
    missatge = client_socket . recv (102) . decode (" utf8 ")
    return missatge

def send_to_socket(missatge):
    formatted_data = bytes (missatge, " utf8 ")
    client_socket.send(formatted_data)

```



```

def create_socket():
    return socket.socket(socket.AF_INET, socket.SOCK_STREAM)

def start_admitting():
    Thread(target = admit).start()

def start_sending():
    while True:
        missatge = input("")
        send_to_socket(missatge)

client_socket.connect(('localhost', 12345))

client_socket = create_socket()

nom = input("nom:")
send_to_socket(nom)

start_admitting()
start_sending()

# SERVER

from threading import Thread
import socket

address = {}
clients = {}

count = 0

def attend_new_client ( conn ):
    Thread ( target = client_connection , args = ( conn , ) ).
        start ()

def income() :
    while True :
        conn , addr = serverSocket . accept ()
        address[ conn ] = addr
        attend_new_client ( conn )

def client_connection ( conn ):

    nom = conn . recv (100) . decode ( " utf8 " )
    clients [ conn ] = nom

    while True :
        broadcast ( nom + ":", conn.recv(100).decode("utf8"))

```

```
def create_socket():
    return socket.socket ( socket . AF_INET , socket .
        SOCK_STREAM )

def broadcast ( prefix , missatge ):
    for sock in clients :
        sock.send(bytes(prefix + missatge,"utf8"))

serverSocket = create_socket ()

serverSocket.bind(( "localhost" ,12345) )
serverSocket.listen(5)

Thread(target = income).start()
```

10 CONCLUSIONS

Ha sigut una pràctica molt útil per entendre els diferents protocols i fer-nos una idea base de com visualitzar una xarxa, és a dir, saber les IP's i el seu tipus (estàtiques, dinàmiques, etc), direccions físiques o MAC, etc, connectar-nos a diversos servidors com poden ser FTP o SSH i realitzar un petit programa servidor-client .

Tots els exercicis ens ha semblat molt interessants ja que, la manera de fer els exercicis ha sigut molt interactiva. A part els conceptes apresos durant la pràctica creiem que ens seran molt útil per poder identificar o tenir una idea d'on poden venir possibles problemes que puguem tenir en un futur en aquesta assignatura o fora.