Pràctica 1. Introducció a les comunicacions

Objectius de la pràctica

L'objectiu d'aquesta pràctica és conèixer aquelles comandes que són d'utilitat des del punt de vista de les xarxes d'ordinadors. Totes aquestes instruccions s'executen des de la consola del nostre ordinador, tot i que existeixen al mercat (amb distribució gratuïta o no) aplicacions que faciliten l'ús d'aquestes. Aquesta pràctica es desenvolupa dins l'entorn de Windows, tot i que les mateixes instruccions o molt similars també s'utilitzen en Linux o MAC OS.

Nombre de sessions

Aquesta pràctica es realitzarà en un màxim de 2 sessions. Un cop finalitzada s'enviarà un informe al professor de pràctiques durant la setmana posterior a través del Campus Virtual de l'assignatura.

Visualització de la xarxa

És molt usual per la majoria dels usuaris d'ordinadors estar connectat a la nostra xarxa local i veure que per alguna raó no tenim connexió a Internet. Quan això passa, el mes senzill de fer és apagar l'ordinador i tornar-lo a encendre. Si el problema persisteix apaguem el router i el tornem a encendre. Si el problema persisteix hem de buscar que és el que està generant aquest error. El primer que volem veure és si tenim connexió amb el nostre router. Sabem la IP del nostre router? Fem el següent:

1.- Cliqueu a l'inici de Windows, a la finestra que hi apareix, escriviu cmd i doneu al retorn. En uns moments apareixerà la finestra de consola de Windows. Si feu servir Linux o MAC, podeu obrir un terminal directament.

Escriviu el següent:

Windows	Linux
• `Ipconfig /all`	• `Ifconfig` o `ip address show`

Si esteu fent servir Linux, la comanda ip correspon a les actualitzacions de kernel i el moviment gradual que es produeix per impulsar les IoT a través de netlink.

Ip ens permet veure també les propietats de les diferents interfícies amb la comanda:

```
>> ip link show
```

També es poden pujar o baixar interfícies de manera similar a ifconfig eth0 up o ifconfig eth0 down simplement fent servir:

```
>>ip link set DEVICE up o ip link set DEVICE down
```

Veureu que, entre tota la informació que apareix, teniu la vostra adreça IP i la màscara. La màscara és un identificador que ens permet conèixer de quina classe és la nostra IP (classe A, B, C, D o E), i si en la nostra xarxa s'ha creat una subxarxa. Es recomana donar una ullada a la vikipèdia per veure les diferents adreces, així com les màscares associades, que corresponen a cada una de les classes (https://ca.wikipedia.org/wiki/Adre%C3%A7a_IP).

Així, per exemple, la classe A va des de la IP 1.0.0.0 fins a la 126.0.0.0 i la màscara agafa, serà un conjunt de bits estructurats de manera idèntica a com els tenim a la IP només que els 8 bits més significatius els trobem a "1". Per tant, si no s'ha fet cap subxarxa la màscara serà 255.0.0.0. Veiem per exemple el cas de l'adreça privada 10.0.0.0. El que tindríem és:

```
IP = 10.0.0.0

Mask = 255.0.0.0
```

Immediatament tindrem una adreça associada a la xarxa (no es pot assignar a cap usuari, ja que serveix per definir la xarxa a la que pertany el teu ordinador) que serà justament la 10.0.0.0 i una adreça de broadcast (per comunicar-se amb tots els usuaris) que serà la 10.255.255.255. Assignem les adreces 10.0.0.1 i 10.0.0.2. La màscara serveix per identificar l'adreça de xarxa. Això es fa fent una AND de la màscara i la IP que tenim. En aquest cas és senzill:

```
10.0.0.2 AND 255.0.0.0 = 10.0.0.0
```

que és l'adreça associada a la xarxa, per tant, el nostre ordinador serà el `0.0.2`

La realització de subxarxes i el seu tractament s'explicarà detalladament a classe de teoria. Normalment per abreviar, el que es sol donar és una compactació de tot plegat, així, si teniu

```
IP : 172.20.0.58

Màscara: 255.255.0.0 (format decimal). En binari 255 = 11111111b
```

Usualment es pot expressar com `IP = 172.20.0.58/16`, ja que en binari, `255.255.0.0` correspon a `11111111.11111111.0.0` es a dir, 16 "1s".

Q1. Quina és la vostra IP?

Feu servir per identificar la vostra adreça IP la comanda abans esmentada.

> Normalment, aquesta IP no és una IP pública, sinó que és privada. 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.

- 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.

Un altra comanda que pot ser interessant de testejar es **netstat**. Netstat s'obté de les paraules NETwork i STATistics. Ofereix estadístiques bàsiques sobre totes les

activitats de la xarxa i informa els usuaris sobre quins ports i adreces s'executen les connexions corresponents (TCP, UDP) i quins ports estan oberts per a tasques.

```
# netstat -nat -n
```

Q2. 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. (help: DHCP?)

En cas que la IP sigui volàtil provarem d'alliberar la IP actual. Per tal de fer això fem:

Windows	Linux
• ipconfig /release • Ipconfig /renew	• **sudo** dhclient -v -r eth0 • **sudo** dhclient -v eth0

En Linux, l'opció -r fa un release o allibera la IP. L'opció -v mostra informació a la pantalla sobre el servidor dhcp i l'arrendament obtingut.

Què ens indica la comanda ipconfig /all després d'executar `ipconfig / release` o `sudo dhclient -v -r eth0`?

Feu servir les comandes per tal d'alliberar l'actual IP i torneu a demanar-ne una. Torneu a fer `ipconfig /all` i constateu si s'ha canviat la vostra ip o bé manteniu encara la que ja teníeu.

Verificació del protocol intern del PC

Arribats a aquest punt podem mirar si el protocol TCP/IP que tenim instal·lat en el nostre PC funciona correctament o hi ha algun problema a la nostra tarja de connexió a la xarxa local (NIC). Per tal de veure això, farem primer una crida al nostre servidor de DNS, o a la porta d'enllaç predeterminada que coneixem quan fem ipconfig. Executem la comanda ping seguida de l'adreça IP, per exemple

- `ping 161.116.95.254`

Q3. Determineu si teniu connexió directa. Desconnecteu ara la vostra connexió a la LAN. Torneu a executar la instrucció. Què passa? 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. Busqueu què és aquesta adreça i perquè serveix.

Verificació de la connexió amb l'exterior

Un cop verificat el funcionament intern, provem si la connexió amb l'exterior és correcta. Accedirem a la pàgina de google per tal de fer la prova, tot i que es pot fer amb qualsevol adreça IP. Farem un ping a l'adreça de google. Això el que fa és enviar un senyal de ECO, que es reenviada per google fins a nosaltres i podem veure el temps que triga en fer-se la connexió. En aquest cas fem:

- `ping www.google.com`

Q4. Verifiqueu que teniu resposta amb google. Quan triguen els paquets en fer tota la ruta complerta (enviar ECO a google i detectar el retorn)? Raona la resposta.

Fins ara hem vist com el servidor (en aquest cas google) respon a la nostra petició de ping. Es possible però que ens interessi conèixer per on han anat passant els paquets, es a dir, la ruta que segueix el datagrama fins arribar a google. Per tal de veure això hem d'utilitzar una nova comanda: `tracert`.

- `tracert www.google.com`

L'equivalent a aquesta comanda en Linux és `traceroute`. `traceroute` ja està instal·lat a Fedora, però s'ha d'instal·lar a Ubuntu. Mireu d'executar-la i si el sistema us indica que no està instal·lada, feu:

```
# sudo apt install traceroute
```

I tot seguit ja podeu executar:

```
# traceroute www.google.com
```

Q5. Indiqueu per quines adreces públiques circulen els datagrames. Apareix el símbol "*"? Que indica?

Coneixement de l'entorn proper

El nostre ordinador es connecta a la xarxa a través d'una xarxa cablejada Ethernet o bé a través d'una xarxa sense fils WiFi. En els dos casos, fem servir un protocol de l'estil 802.x on s'han d'especificar les adreces MAC del PC origen i destí.

Q6. Què és una adreça MAC? Puc tenir adreça MAC i no adreça IP? Raona la resposta

Feu servir la comanda `ipconfig` per identificar la vostra adreça MAC. Quants bits té? A aquesta adreça es sol anomenar també com adreça física, mentre a l'adreça IP es també coneguda com adreça lògica. Per fer qualsevol connexió amb un altre PC, que estigui a la nostra xarxa local o en qualsevol altre lloc, necessitarem dos adreces IP (origen i destí) i dos adreces MAC, especificades al protocol 802.x. La pregunta que ens fem és la següent, la IP tenim clar com es pot obtenir, però com podem saber l'adreça MAC? El protocol que ens dona aquesta informació és el ARP (Address Resolution Protocol), el funcionament del qual s'explica detalladament a teoria però que podem resumir en que el PC origen envia un paquet on s'especifica la IP origen i la IP destí, la MAC origen i es demana la MAC destí, seria una petició de l'estil:

"hola, sóc el node amb IP A, vull connectar amb el node amb IP B, la meva MAC és C, però no conec la MAC del node destí, Que me la podria dir el node amb IP B?"

Si el node destí esta a la mateixa xarxa LAN, ell mateix respondrà a la pregunta enviant un ARP response, que seria una cosa com

"hola, jo soc el node amb IP B, responc al node amb IP A i MAC C, la meva MAC és D"

A partir d'aquí el node ja pot enviar la informació (e-mail, Telnet, ftp,...) al node destí. En cas que el node destí no estigui en la nostra xarxa local, qui respon al ARP

request és el Router de sortida, dient una cosa com "hola, node amb IP A i MAC C, envia el paquet a la IP B i fes servir la MAC F", que correspon amb la MAC del router, el paquet arriba al router i aquest ja s'encarrega d'enviar la informació a través d'internet.

El PC sol guardar les darreres adreces MAC que ha fet servir. Aquesta taula és dinàmica i per tant no hi ha cap dada fixa. Podem visualitzar la taula i modificar-la fent servir la comanda arp. Les opcions més interessants des de Windows són:

> `arp –a` mostra la taula dinàmica

> `arp –s` agrega una entrada estàtica associant-li una ip. Ex:

> `arp –s 161.11.1.2 00-aa-00-bb-00-cc` (mireu d'associar un element real, ja que pot donar problemes en cas contrari)

> `arp –d` elimina el host especificat per la IP. Amb un * elimina totes les entrades

Quantes entrades té la vostra taula ARP?

Q7. Proveu d'esborrar tota la taula ARP. Feu servir `arp -h` per veure totes les opcions que ens proporciona aquesta comanda. Què passa? Torneu a obrir la consola i determineu la mac del router de sortida.

Estadística de xarxa

La comanda `netstat` (network statitstics) és una eina que ens indica les connexions actives del nostre PC. Quan executem `netstat` des de consola visualitzem el protocol que es fa servir, les taules de Routing, les estadístiques de les interfícies utilitzades i l'estat de la connexió.

Executeu de nou des de la consola la següent comanda:

- `netstat –h`

aquesta comanda ens indica totes les opcions que podem gaudir. Destaca la bàsica , `netstat –a` que mostra totes les connexions i ports que es fan servir. Algunes d'aquestes opcions requereixen executar la comanda en mode Administrador, si no és possible fer-ho a la sala d'ordinadors de la facultat (no teniu drets), feu-lo a casa.

Q8. En aquest cas, obriu una consola en aquest mode (botó dret opció Executar com Administrador) i proveu les diferents opcions. Que fa la opció –r? Que és la mètrica?

Connexions amb servidors

Les comandes bàsiques que tenim per connectar-nos amb servidors són:

- Telnet: protocol que permet la connexió remota a una altra màquina.
- ftp: protocol que permet la transferència de fitxers de un servidor remot
- ssh: Similar al Telnet però molt més segur. L'intercanvi de dades amb Telnet (login i password) es transmeten per la xarxa com a texte pla (cadenes de text sense xifrar). Ssh permet la comunicació segura entre màquines.

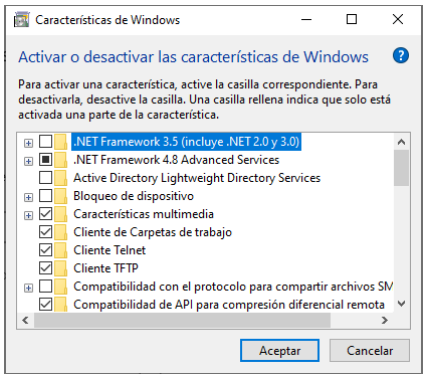
Telnet

Q9. Executem des de la consola la comanda Telnet. Ens connectarem amb el servidor del "National Institute of Standards and Technology", en Boulder, Colorado, USA. La connexió la farem de la següent forma:

- `telnet time-A.timefreq.bldrdoc.gov 13`

La resposta del servidor és la data complerta (dia i hora) ja que ens hem connectat al servei "time of the day" que moltes màquines UNIX executen diàriament.

Comentari per la gent de Windows: Després de barallar-te, pot ser que la consola t'indiqui que Telnet NO es reconeix com una comanda del sistema. La raó és que Windows no les te habilitades. Habiliteu-les clicant a Inici ➔ Configuració➔Aplicacions. Escriviu amb bona lletra "activar o desactivar las características de Windows". S'obrirà una finestra com aquesta:



Habiliteu les comandes necessàries en cada cas.

Q10: Torneu a provar la connectivitat de la comanda anterior. Indiqueu on us heu connectat i que heu rebut.

Telnet és una comanda vulnerable, ja que executa una connexió oberta. Per aquesta raó, en ocasions el Firewall de Windows no ens permet la connexió, donant un error:

```
C:\Users\mlope>a conexión con el host.
C:\Users\mlope>telnet towel.blinkenlights.nl
Conectándose a towel.blinkenlights.nl...No se puede abrir la conexión al host, en puerto 23: Error en la conexión
```

ssh

De la mateixa forma que el Telnet, ssh ens permet connectar-nos de manera remota a una altra màquina. A diferència del Telnet, on la connexió és oberta, ssh ens permet connectar-nos amb una certa seguretat.

Ssh permet la possibilitat de redirigir transit de sistemes amb X Windows i poder executar entorns gràfics de forma remota, sempre i quan tinguem un servidor X corrent a la màquina host. A diferència de Telnet, ssh no es pot executar directament des de una consola de Windows. No es reconeix la comanda. Tenim dues opcions, o bé passem a l'entorn de Linux o bé instal·lem una aplicació que emula una consola de Linux. Una de les aplicacions gratuïtes que més es fa servir

per fer aquesta emulació és el programa PuTTY. Una altra opció és fer servir el programa MobaXterm. Aquest darrer programa emula un terminal de linux amb una corba d'aprenentatge prou ràpida.

Q11. Exercici de connexió remota fent servir ssh:

Obriu un PC en entorn Linux. Si treballeu en Windows utilitzeu el programa MobaXterm. Mireu quina IP té assignada aquest PC. A diferència de Windows, Linux fa servir la comanda ifconfig per mostrar las adreces MAC i IP. Des de un altre ordinador (Linux) executeu la comanda ssh de la següent forma:

- ssh –X usuariHost@IP_host

des de consola es demanarà el password de l'usuari, introduïu-lo. Executeu qualsevol aplicació de forma remota.

Q12

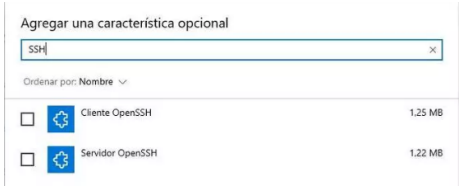
En Windows feu:

Exercici 1: Instal·lació del SW MobaXterm.

1. Clica a la icona de `Servers`
2. Inicia un servidor de ssh. El temps que romandrà obert el servidor és per defecte de 360 segons
3. Des de la consola de MobaXterm clica sobre `Session` i clica sobre la opció SSH.
4. Podem connectar-nos al nostre propi Servidor (si encara no han passat els 360 segons) posant el nostre nom d'usuari i la IP `127.0.0.1`. Ens demanarà el nostre propi password.
5. Si ho feu en parelles, podeu mirar de connectar-vos entre vosaltres.

Exercici 2. Treballant només amb Windows:

1. Windows 10 i 11 incorporen el servei OpenSSH, però ens caldrà instal·lar-ho. Aneu a Inici ➔ Configuració ➔ Aplicacions
2. En Aplicacions us heu de quedar a Aplicacions i Característiques. A la finestra principal, sota de Aplicacions i Característiques aneu a Característiques opcionals.
3. Cliqueu sobre +Agregueu una Característica i podeu escriure OpenSSH. Instal·leu el client i el servidor



4. En el buscador poseu `services.msc`. Feu doble clic en OpenSSH Autentication Agent i en OpenSSH SSH server i habiliteu-los, escollint la opció de Automàtic.
5. En el cas del servidor el podeu Iniciar l'estat del servei quan el vulgueu provar.

6. Obriu el Windows Power Shell. Al buscador només cal escriure Windows Power Shell i us mostrarà l'executable. Obriu-lo.
7. Executeu la comanda Get-Service sshd, us indicarà si el servei està funcionant o està parat. Si està parat, inicieu-lo (veure punt 5)
8. Executeu ssh usurariHost@IP_host, en aquest cas el vostre nom d'usuari de Windows i la IP 127.0.0.1
9. Si ho feu en parelles podeu mirar de connectar-vos entre vosaltres
10. Recordeu detenir el servidor SSH.

FTP

A diferència dels anteriors, FTP és un protocol que permet transferir fitxers de servidors de FTP. Justament la seva utilitat rau en tenir un accés públic on pujar o descarregar fitxers comuns a diferents usuaris sense la necessitat de enviar-los per e-mail. Tenen molta utilitat quan els fitxers són de una mida prou gran com per fer que la transmissió per e-mail sigui lenta o quan utilitzem servidors de e-mail que limiten la quantitat de MBytes a indexar en els correus electrònics. Des de la consola de Linux, podeu obtenir informació de la comanda ftp posant:

- man ftp

Ens connectarem al servidor de rediris de forma anònima. Des de consola fes:

- ftp ftp.rediris.es

en aquest servidor trobareu una sèrie de programes de distribució gratuïta. Abans de tot us demanarà usuari i password. En usuari poseu anonymous, en la part de password podeu posar qualsevol cosa.

Les opcions de ftp les podeu veure posant

ftp> help

Normalment les més utilitzades són get o mget per descarregar fitxers i put per pujar fitxers al servidor. En aquest cas, rediris és la xarxa espanyola per a la interconnexió de recursos informàtics de les universitats i centres d'investigació.

Q13 Des de MobaXterm podeu activar el servidor i el client de FTP tal i com heu fet a l'exercici anterior. Descarregueu algun dels fitxers que proporciona el servidor. Podeu pujar fitxers al servidor?

Des del terminal: Executeu ipconfig i també ifconfig. Expliqueu les diferències i similituds.

Dintre de MobaXterm instal·leu el paquet Lynx. Feu servir apt-get install lynx.

Executeu la següent comanda:

Lynx http://www.ub.edu

Posteriorment executeu la comanda:

Lynx –dump http://www.ub.edu

Expliqueu que fa i quina utilitat pot tenir.

Sockets i Aplicació Pràctica

Es proposa que munteu un xat entre vosaltres. Per tal d'assolir aquest objectiu, un proporcionem uns exemples que poden fer-se servir a l'hora de programar aquest xat. Podeu fer servir la classe socket per al client i la classe ServerSocket per al servidor.

Link sockets python:

https://realpython.com/python-sockets/

https://pymotw.com/3/socket/tcp.html

Un cop finalitzat el programa, feu una prova amb el professor de l'aula per tal d'avaluar la tasca.

Informe de la pràctica

L'informe d'aquesta pràctica ha de constar de:

1.- Objectius de la pràctica

2.- Resposta a les diferents qüestions que en ella es plantegen als alumnes

3.- Explicació de la feina realitzada al laboratori

4.- Conclusions