

Simulacre prova final UF1 Xarxes

1.-Respon les següents preguntes:

a) ¿Per a què serveix aquest producte: <https://cablematic.com/ca/productes/convertidor-de-fibra-optica-1000-mbps-multimode-de-lc-a-rj45-a-550m-UF041> ?

b) Més en concret, ¿quina diferència hi ha entre els estàndards "1000Base-TX" i "1000Base-SX" (vistos a classe), presents a la seva descripció?

bII) ¿Què signifiquen les sigles "UTP" i "LC" (vistes a classe), presents a la seva descripció?

c) ¿Sabries dir si el següent transceptor és compatible amb el producte anterior (o no) i per què <https://www.prolabs.com/products/transceivers/huawei/sfp/1000base/sfp-ge-sx-mm850-a-c> ? **Pista:** has de comprovar que les dades indicades a la taula "Technical specification" concorden amb la descripció i dades tècniques mostrades a l'enllaç proporcionat a l'apartat a)

d) Indica l'enllaç dins d'alguna botiga online d'un cable de fibra òptica compatible amb el transceptor anterior **Pista:** t'has de fixar que ambdós productes tinguin el mateix tipus de connector i que el cable sigui d'un mode MM compatible amb la llargària i l'amplada de banda màxima admeses pel transceptor

e) D'altra banda, ¿per a què (i com) faries servir aquest producte: <https://cablematic.com/ca/productes/ultra-power-over-ethernet-poe-injector-ieee8023afat-101001000mbps-fins-50vdc-RA021> ? ¿Admet PoE+?

2.-a) A la web <https://iperf.fr/iperf-servers.php#public-servers> hi ha llistats diversos servidors Iperf3 disponibles a Internet. Tria qualsevol d'ells (fixa't en quin port estan escoltant!) per fer un test que mesuri el "throughput" (també conegut com "bitrate" o "bandwidth") actual del teu ordinador en relació a aquest servidor d'Internet.

aII) Repeteix el procés descrit a l'apartat anterior però ara amb un altre servidor diferent dels indicats al llistat. ¿Hi ha diferències significatives entre els valors del "throughput" obtinguts en cada test? ¿Per què?

b) ¿Quina comanda faries servir (i com) per mesurar la latència "two-way" (RTT) entre el servidor Iperf3 triat al primer apartat d'aquest exercici i el teu ordinador? Fes-ho i, a partir d'aquí, calcula el valor resultant del BDP.

bII) ¿Quina diferència hi ha entre el RTT i el "one-way delay" i perquè no se'n pot deduir un de l'altre?

c) Registra't (gratuïtament) en el lloc web <https://perfops.net>. Un cop fet això, inicia sessió en el seu panell web online, vés a l'opció del menú "Tools->Latency benchmark" i allà escriu "elpuig.xeill.net" com a nom de "host". ¿Quin és el significat del resultat que obtens en fer el test?

cII) Vés ara a l'opció del menú "Tools->Network utilities", escriu allà "elpuig.xeill.net" com a nom de "host" i "Portugal" com a "location" i executa el test "mtr". ¿Què volen dir les adreces IP que apareixen com "???" ?

d) ¿Quina comanda faries servir (i com) per mesurar el número i percentatge de paquets perduts entre l'ordinador "www.marca.com" i el teu ordinador?

3.-Crea amb el VirtualBox:

- *Una màquina virtual anomenada "MaqA" amb 2GB de RAM i una sola tarja de xarxa en mode "xarxa interna" executant un sistema Server (Ubuntu o Fedora, a escollir)
- *Una màquina virtual clon de l'anterior anomenada "MaqB" que també tingui una sola tarja de xarxa en mode "xarxa interna"
- *Una màquina virtual clon de l'anterior anomenada "MaqC" però que tingui dues tarjes de xarxa: una en mode "xarxa interna" (la enp0s3) i una altra en mode "adaptador pont" (la enp0s8)

a) Arrenca "MaqA". Assigna a la seva tarja de xarxa la IP 192.168.3.1/24 i fes que la seva porta d'enllaç per defecte sigui 192.168.3.3 i el servidor DNS principal a usar sigui 9.9.9.9. Tot de forma estàtica mitjançant "systemd-networkd" (vigila que, si estàs a Ubuntu, cap configuració Netplan no et molesti). Confirma que hagi indicat bé la configuració demanada observant la sortida de la comanda `networkctl -n 0 status` Apaga finalment la màquina "MaqA".

b) Arrenca "MaqB". Estableix la configuració de la seva tarja de xarxa per a què sigui dinàmica (és a dir, s'obtingui a través d'algun servidor DHCP -encara per implementar-) també mitjançant "systemd-networkd". Confirma que hagi indicat correctament la configuració demanada (tot i que encara no hagi pogut obtenir cap dada de xarxa perquè no hi ha d'on agafar-les, és normal) observant la sortida de la comanda `networkctl -n 0 status` Manté la màquina encesa

c) Arrenca "MaqC". Assigna a la seva tarja de xarxa interna la IP 192.168.3.3/24 (però cap porta d'enllaç) de forma estàtica mitjançant "systemd-networkd" i escriu, a més, les directives adients dins del fitxer ".network" per tal d'activar en ella la funcionalitat de servidor DHCP; concretament, fes que ofereixi IPs en el rang 192.168.3.10-192.168.3.20, que s'ofereixi com a porta d'enllaç ella mateixa i que ofereixi com a servidor DNS la IP 9.9.9.9. Després de reiniciar el servei "systemd-networkd" així configurat a "MaqC", executa llavors la comanda `sudo networkctl reconfigure enp0s3` a "MaqB" i tot seguit confirma que hagi establert correctament la seva configuració de xarxa tornant a observar la sortida de la comanda `networkctl -n 0 status` a "MaqB". Un cop fet, pots apagar la màquina "MaqB" però mantingues encesa la màquina "MaqC".

4.-a) Arrenca la mateixa màquina "MaqA" de l'exercici anterior. Atura el servei "systemd-networkd" i inicia el servei "NetworkManager". Utilitza ara l'eina `nmcli` per assignar a la tarja de xarxa de la màquina la IP 192.168.3.1/24, i fer que la seva porta d'enllaç per defecte sigui 192.168.3.3 i que el servidor DNS principal a usar sigui 9.9.9.9. Confirma que hagi indicat bé la configuració demanada observant la sortida de la comanda `nmcli -f IP4.ADDRESS,IP4.GATEWAY,IP4.DNS device show enp0s3` Un cop fet, pots apagar la màquina "MaqA".

b) Arrenca la mateixa màquina "MaqB" de l'exercici anterior. Atura el servei "systemd-networkd" i inicia el servei "NetworkManager". Utilitza l'eina `nmcli` per establir la configuració de la tarja de xarxa de la màquina per a què aquesta sigui dinàmica (és a dir, s'obtingui a través de DHCP). Confirma que hagi indicat bé la configuració demanada observant la sortida de la comanda `nmcli -f IP4.ADDRESS,IP4.GATEWAY,IP4.DNS device show enp0s3` Un cop fet, pots apagar la màquina "MaqB" però mantingues la màquina "MaqC".

NOTA: Pots forçar rebre la configuració DHCP executant `nmcli con down nomConnexió && nmcli con up nomConnexió`

5.-a) Crea dins de la carpeta `/etc/systemd/network` de la màquina "MaqC" de l'exercici anterior un nou arxiu amb el nom "10-lerele.link" que tingui el següent contingut i tot seguit reinicia la màquina completa. ¿Quines quatre dades del Nivell 2 són les que modifica aquest fitxer de configuració i amb quina/es comanda/es vistes a classe podries comprovar cadascun d'aquests nous valors? Apaga finalment la màquina

NOTA: Recorda que el nom de l'arxiu ha de començar per un nombre petit perquè tots els arxius ".link" existents (tant dins de `/usr/lib/...` com dins de `/etc/...`) es llegeixen en ordre segons el seu nom i s'aplica la primera configuració trobada.

```
[Match]
MACAddress=08:00:27:xx:xx:xx <--Indica aquí l'adreça MAC de la tarja enp0s8
[Link]
Name=pepe0
MTUBytes=9000
MACAddress=08:00:27:65:43:21
WakeOnLan=magic
```

b) Substitueix la línia `MACAddress=...` de la secció `[Link]` anterior per la línia `MACAddressPolicy=random` i reinicia de nou la màquina. ¿Quin canvi passa i digues quina comanda has fet servir per saber-ho? **Pista:** pots consultar `man systemd.link`

6.- Respon les següents preguntes:

a) Si vols saber si tens el port 3306 "obert" (és a dir, "escoltant") al teu sistema, ¿què hauries de fer? ¿I per confirmar que és el programa MySQL qui està al darrera d'aquest port i no un altre programa?

aII) ¿Quin és el significat de la sortida del conjunt encadenat de comandes següent, i en quina situació penses que seria útil executar-lo?: `ss -tnH | tr -s " " | cut -f5 -d " " | cut -f1 -d: | wc -l` ¿I el significat d'aquest altre conjunt de comandes: `ss -tnH "dport = :22 or dport = :443" | tr -s " " | cut -f5 -d " " | cut -f1 -d: ?`
Pista: consulta les pàgines del manual de les diferents comandes involucrades

b) Digues quina comanda `ncat` de tipus servidor concreta hauries d'executar per tal de poder oferir...

- *...un shell Bash remot ...
- *...encès de forma permanent (és a dir, que no s'aturi quan es desconnecti un client)...
- *...només disponible pel client que tingui una determinada adreça IP (la teva, que suposarem fixa)...
- *... i que funcioni via UDP (en lloc de TCP, que és el normal)

Digues també quina comanda `ncat` de tipus client hauries d'executar per tal d'accedir a aquesta funcionalitat

c) Digues quina comanda `nmap` concreta hauries d'executar per tal de...

- *...saber quin dels ports entre el 1 i el 1000 que té oberts la màquina "www.hola.com"...
- *...a més de saber també els programes associats a aquests ports...
- *...i la versió del sistema operatiu que aquesta màquina està executant

cII) Explica...:

... pas a pas què fa cadascuna de les comandes següents (incloent una descripció de tots els paràmetres indicats i de les expressions regulars implicades) i quin és el resultat final obtingut:
`nmap -Pn -n -p- ip.del.teu.router -oG - | grep -oP "\d{1,5}/open" | cut -f1 -d "/" | tr "\n" ","`

... quina informació extra mostra el paràmetre `--packet-trace` de Nmap i per què és interessant

... per a què faries servir la següent comanda: `watch -n 10 nmap -n -sn ip.de.la.teva.xarxa/mascara`

d) Digues què fan cadascuna de les següents comandes (explicant també els seus paràmetres) i respón:

<code>nping --arp --arp-request -c 1 192.168.1.1</code>	¿A quina altra comanda seria equivalent?
<code>nping --arp --arp-request -c 1 192.168.1.0/24</code>	¿A quina altra comanda seria equivalent?
<code>nping --icmp --icmp-type 8 -c 1 www.hola.com</code>	¿A quina altra comanda seria equivalent?
<code>nping --udp -p 321 -c 1 --data-string "hola" 127.0.0.1</code>	¿Quina és la resposta que es rep?
<code>nping --tcp --flags syn -p 80 -c 1 www.hola.com</code>	¿Quina és la resposta que es rep?
<code>nping --tcp-connect -p 80 --rate 10 -c 90 www.hola.com</code>	¿Què mostra en paral·lel <code>watch -n 1 ss -tn?</code>

La llibreria "Global Socket Toolkit", implementada en diversos programes que de seguida estudiarem, permet establir una connexió TCP a través d'Internet entre dos sistemes funcionant darrera d'un tallafocs NAT (és a dir, amb adreces IP privades!). Per aconseguir això utilitza com a nus d'"empalmament" la xarxa gratuïta "Global Socket Relay" (GSRN), la qual connecta entre sí les màquines que coneixen el mateix secret (en lloc de fer servir ni l'adreça IP ni el número de port de cadascú). Aquest secret s'utilitza per derivar-ne identificadors de sessió TLS temporals, de forma que el secret no abandona mai cada màquina i la GSRN només veu trànsit xifrat (aconseguint així que la connexió entre els dos extrems sigui confidencial i segura).

7.-Arrenca dues màquines virtuals qualssevol però que tinguin la seva respectiva tarja de xarxa en mode NAT (això és important!!) i segueix els següents passos per instal·lar el Global Socket Toolkit a cadascuna:

* A Ubuntu: Executa `sudo apt install gsocket`

* A Fedora: Executa `sudo dnf install git gcc make autoconf automake openssl-devel`
`bash -c "$(curl -fsSL https://gsocket.io/install.sh)"`
`cd gsocket && sudo make install`

a) Executa les següents comandes i digues què fan i per a què serveixen els paràmetres indicats (com a ajuda pots consultar *man gs-netcat*):

A la màquina A: `gs-netcat -li`

A la màquina B: `gs-netcat -i` i tot seguit executar qualsevol comanda com per exemple: `echo 'hola';id; exit`

NOTA: Una altra forma d'aconseguir quelcom similar però en aquest cas de forma no interactiva seria fer per exemple:

A la màquina A: `gs-netcat -l -e "echo 'hola';id; exit"`

A la màquina B: `gs-netcat`

b) Executa les següents comandes i digues què fan i per a què serveixen els paràmetres indicats (com a ajuda pots consultar *man gs-netcat*):

A la màquina A: `gs-netcat -s unsecret -lr > unfitxer.txt`

A la màquina B: `gs-netcat -s unsecret < unfitxer.txt`

NOTA: Una altra comanda del GST més especialitzada en el trànsit de fitxers és *blitz*, utilitzada d'aquesta manera:

A la màquina A (la que rebra els fitxers): `blitz -l`

A la màquina B (la que els enviarà): `blitz /usr/share/* /etc/*`

c) Executa les següents comandes i digues què fan i per a què serveixen els paràmetres indicats (com a ajuda pots consultar *man gs-netcat*). Important: a "Màquina A" (tot i que podria ser qualsevol altra màquina, però per no haver de tenir tres màquines virtuals en marxa) hauràs de tenir, en aquest apartat, a més, un servidor SSH en marxa (tot i que podria ser de qualsevol altre tipus):

A la màquina A: `gs-netcat -l -d 127.0.0.1 -p 22`

A la màquina B: `gs-netcat -p 2222` i, en un altre terminal, `ssh -p 2222 usuari@127.0.0.1`

Pista: Entre màquina A i B s'estableix un "túnel" a través de la GSRN gràcies a les comandes *gs-netcat* respectives. A la màquina A, aquesta comanda *gs-netcat* el que fa és reenviar tot el que li arriba al port local 22 (on se suposa que hi ha un servidor SSH en marxa). A la màquina B, aquesta comanda *gs-netcat* obre un port local, que servirà com a punt d'entrada al túnel, el qual és utilitzat per la comanda client *ssh*. D'aquesta manera, el client *ssh* connecta a través del túnel amb el servidor SSH de l'altre extrem (fent servir un usuari existent en aquest servidor, òbviament). En altres paraules: aquest és un exemple pràctic de com accedir des d'Internet (a través de la GSRN) a un servidor que només està escoltant realment de forma local (o com a molt, dins d'una xarxa privada)

NOTA: El GST incorpora més comandes interessants a més de les vistes en aquest exercici (com *gs-mount* o *gs-sftp*). Totes elles tenen la seva corresponent pàgina del manual

NOTA: D'altra banda, altres paràmetres interessants de la comanda *gs-netcat* són *-S* o *-D* (ambdós combinats amb *-l*)

NOTA: També existeix una versió del GST mínima que només inclou *gs-netcat* i ja està, directament descarregable de <https://www.gsocket.io/deploy>

NOTA: El codi per implementar un servidor "relay" de la GSRN es troba a <https://github.com/hackerschoice/gsocket-relay>

NOTA: En el cas d'haver instal·lat GST amb la comanda `sudo make install`, per desinstal·lar-la caldrà fer (des de dins de la mateixa carpeta "gsocket"), la comanda `sudo make uninstall`