Comandes de xarxa

Conceptes bàsics de xarxes (direcció IP, màscara, porta d'enllaç i servidor DNS):

¿Què necessita un ordinador per poder-se comunicar amb un altre? A més del hardware adient, necessita un sistema operatiu que inclogui una "pila de protocols" (implementats en software, doncs) que realitzin i gestionin tots els passos de la comunicació (l'establiment de la connexió, l'intercanvi d'informació entre els extrems, el control dels possibles errors, el procés de desconnexió, etc). Tant a les xarxes cablejades de tipus Ethernet com a les inalàmbriques de tipus WiFi s'utilitza la mateixa pila software (ja incorporada en tots els sistemes operatius actuals per defecte): l'anomenada "pila TCP/IP". No obstant, a més de tenir la pila, cada sistema ha de tenir configurats certs paràmetres per comunicar-se amb l´exterior:

*Direcció IP : Identifica una màquina. Hi ha dos formats, la IPv4 (que ofereix 2^{32} direccions diferents, amb la forma nº.nº.nº.nº, on "nº" pot valer entre 0 i 255 -és a dir, correspon a un byte) i la IPv6 (que n'ofereix $2^{48,}$ amb la forma nº:nº:nº:nº:nº:nº on "nª també és un byte però sol escriure's en format hexadecimal). Aquí només estudiarem IPv4, la més usada -encara- avui dia.

Com que la IPv4 no ofereix prou direccions diferents per tots els dispositius del món, hi ha certs rangs d'IPs que són privats (és a dir, rangs que són els únics que es poden usar dins de les xarxes administrades per nosaltres -també anomenades "LAN", de "Local Area Network"- sense perill que es solapin amb les IPs assignades a màquines d'altres LANs -com poden ser la del veí, la de l'oficina del costat, etc-). Els rangs privats són aquests:

-Classe A 10.0.0.0-10.255.255.255
-Classe B: 172.16.0.0-172.31.255.255 (i també 169.254.0.0 – 169.254.255.255)
-Classe C: 192.168.0.0-192.168.255.255

Qui assigna les IPs públiques (és a dir, les IPs directament accessibles a Internet per tothom i, per tant, sense possibilitat de poder-se repetir) és l'organització ICANN (antiga IANA): http://www.icann.org/tr/spanish.html a través de les seves delegacions territorials (RIPE a Europa, ARIN a Amèrica del Nord, etc). Concretament, ICANN presta "borses" de direccions IP a les diferents companyies de telecomunicacions, les quals al seu torn lloguen aquestes als seus clients respectius per tal de donar-los accés a Internet.
NOTA: ICANN també s'encarrega d'assignar els noms de domini i els números de ports.

*Màscara de xarxa: Ubica la direcció IP d'una màquina dins d'una determinada xarxa. Per aconseguir això, defineix quina part de la IP correspon a la direcció de xarxa i quina al número identificador de l´equip concret dins d'aquesta xarxa. Serveix, doncs, per saber si una determinada màquina pertany (o no) a la mateixa xarxa que una altra. Les màscares, al igual que les direccions IPv4, estan formades per quatre números que poden valer entre 0 i 255 cadascun. No obstant, de totes les màscares eventualment possibles, només hi ha tres que s'utilitzin habitualment, les anomenades "de classe A", "de classe B" i "de classe C". Són les següents:

-Classe A: 255.0.0.0 (també es pot indicar amb un "/8" rera la IP que acompanyi)
-Classe B: 255.255.0.0 (també es pot indicar amb un "/16" rera la IP que acompanyi)
-Classe C: 255.255.255.0 (també es pot indicar amb un "/24" rera la IP que ")

La part de la màscara on tot són uns binaris (és a dir, en el cas de les màscares de classe A, B o C, els bytes que valen "255") indica quina part de la direcció IP associada es correspon a la xarxa a la què pertany la màquina en qüestió, i l'altra part de la màscara es correspon a l'identificador propi d'aquella màquina. Per exemple, una màquina amb direcció IP + màscara 192.168.10.3/24 pertany a la xarxa "192.168.10" amb identificador "3" i l'ordinador 192.168.10.4/24 pertanyeria a la mateixa xarxa (i per tant, es podria comunicar directament amb l'anterior) però tindria l'identificador "4". En canvi, si aquest darrer tingués la direcció IP + màscara 192.168.10.4/16, llavors la seva xarxa seria la "192.168" (i el seu identificador personal "10.4") i, per tant, ja no pertanyeria a la mateixa xarxa que la primera màquina.

NOTA: Cal aclarir que, en realitat, les xarxes no es nombren com hem explicat al paràgraf anterior sinò que tenen un identificador que és una direcció IP pròpiament dita. Aquesta **IP "de xarxa"** es forma simplement afegint zeros a la dreta de la part de la xarxa marcada per la màscara fins arribar a completar una IP. Per exemple, si un ordinador té la direcció IP + màscara 192.168.10.3./24, la forma correcta d'expressar el que s'ha explicat al paràgraf anterior és dir que aquest ordinador pertany a la xarxa "192.168.10.0/24" (i té l'identificador "3" -o també, directament, "192.168.10.3/24"-). Igualment, si un ordinador té la direcció IP + màscara 192.168.10.4/16, pertany a la xarxa "192.168.0.0/16" i té l'identificador "10.4" (o també, directament, "192.168.10.4/16"). És important remarcar que aquesta IP "de xarxa" és una direcció que no té ni pot tenir cap màquina en concret ...és un identificador global de la xarxa com a tal i no una direcció IP a implementar físicament en cap lloc.

Tenint en compte els rangs d'IPs privades existents anteriorment comentats, podem deduir fàcilment que podrem tenir només una xarxa de classe A privada (la 10), fins 16 xarxes privades independents de classe B (172.16,172.17,...) i fins 256 xarxes privades independents de classe C (192.168.0, 192.168.1,...).

Finalment, dir que per cada xarxa existeix una direcció IP especial anomenada **IP "de broadcast"** que serveix no per identificar una màquina concreta dins d'aquesta xarxa en qüestió sinó per indicar literalment "totes les màquines d'aquesta xarxa". Aquesta IP es forma indicant tos d'uns binaris a la part de la IP que queda "a la dreta" quan es divideix amb la màscara (és a dir, la part que correspon a l'identificador de màquina). Per exemple, la IP de broadcast a la què l'ordinador 10.24.56.42/8 hauria d'enviar un missatge per a què arribés a tothom de la seva xarxa seria la 10.255.255.255.

Una altra IP especial és l'anomenada **IP "loopback"**, la qual pot ser qualsevol de la xarxa 127.0.0.0/8 encara que normalment es fa servir sempre la direcció 127.0.0.1. Aquesta direcció IP representa sempre la pròpia màquina, independentment de què tingui (o no) tarjes de xarxes amb altres direccions IP configurades. És a dir, és una direcció IP que permet comunicar les aplicacions d'una màquina entre sí sense què cap dada surti a l'exterior (d'aquí el nom de "llaç"). La direcció IP "loopback" està associada sempre a una tarja fictícia inventada pel sistema operatiu. Veurem la seva utilitat més endavant.

*Porta d´enllaç/passarela/gateway/router: Per a què qualsevol màquina pertanyent a una xarxa pugui comunicar-se amb una altra màquina pertanyent a una altra xarxa ha d'haver-hi entremig un dispositiu especialitzat que faci de "passarela" entre les dues xarxes en qüestió (també se sol anomenar "enrutador", o en les paraules en anglès: "gateway" i "router", respectivament). Aquest dispositiu ha de tenir, doncs, com a mínim dues tarjes de xarxa: una a cada xarxa de les que vol comunicar (i internament realitzarà les connexions necessàries per vincular-les). No obstant, no és suficient amb tenir aquest dispositiu funcionant: cada màquina de qualsevol de les xarxes a interconnectar ha de tenir gravada, a més, la direcció IP de la tarja de l'enrutador que tingui "a la seva banda" per tal de saber a qui s'haurà de connectar cada cop que vulgui "sortir" de la seva xarxa per a que li ajudi a arribar a

qualsevol altra xarxa remota. És per això que als "routers" se'ls anomenen també "porta d'enllaç".

NOTA: Si la xarxa de destí desitjada no està directament connectada a la porta d'enllaç que tenim configurada, existeixen protocols d'enrutament específicament utilitzats pels enrutadors per tal de comunicar-se entre ells i així esbrinar quina és la millor ruta per aconseguir fer arribar la informació al seu destí final encara que sigui remot. Internet, de fet, no és més que un conjunt de diferents xarxes interconnectades entre sí mitjançant diferents routers.

*Servidors DNS predefinits: Per tal de connectar amb una màquina remota, una màquina d'origen només necessita saber la direcció IP de la primera (i, si aquesta fos d'una xarxa diferent a la seva, tenir configurada una porta d'enllaç). No obstant, pels sers humans no és fàcil recordar direccions IPs: no és el mateix utilitzar com a identificador d'una màquina la seva IP (la qual podria ser una qualsevol com 142.33.126.97) que un nom (com aquest: "www.hola.com").

Per poder fer servir noms en comptes de direccions IPs a l'hora de connectar amb màquines remotes (ja sigui navegant per Internet, accedint via SSH, fent pings, etc, etc) existeixen els anomenats servidors DNS públics, els quals no són més que ordinadors ubicats a Internet que ofereixen gratuïtament un servei de "traducció" de noms a direccions IPs. Aquests servidors DNS són propietat de diferents empreses (generalment de l'àmbit de les telecomunicacions: Google, Telefonica ... -es pot consultar una llista força completa a http://public-dns.info-) però són tots equivalents entre sí perquè funcionen com a rèpliques-clon uns dels altres.

Qualsevol màquina que vulgui utilitzar qualsevol d'aquests servidors DNS caldrà que tingui configurat exactament quin d'aquests servidors en concret utilitzarà sempre per fer les consultes que necessiti. D'aquesta manera, cada cop que qualsevol programa d'aquesta màquina (navegador, ping, etc) rebi de l'usuari el nom d'una màquina remota a la qual s'haurà de connectar, aquest programa primer realitzarà la consulta al servidor DNS que tingui configurat el sistema per esbrinar la direcció IP de la màquina remota en qüestió, i un cop esbrinada, només llavors procedirà a realitzar la connexió demanada pròpiament dita.

(Alguns) protocols de la pila TCP/IP:

La pila TCP/IP es diu així perquè està formada per un conjunt de capes independents que treballen de forma coordinada en nivells, per tal d´aconseguir la comunicació entre les màquines. És la filosofia de “divideix i venceràs”: que cada element faci una cosa, però la faci bé (de forma modular). Concretament, les capes TCP/IP presents a una màquina són:

*Capa d´enllaç/física: S'encarrega de la generació, transport i recepció de les senyals físiques (elèctriques, electromagnètiques, etc) entre els extrems d'una connexió segons els estàndards de telecomunicacions establerts, i a més, de l'establiment i manteniment de la comunicació extrem a extrem. Els switchos només treballen fins aquí (ignoren la resta de conceptes que apareixen a capes superiors)

En aquest nivell és on té rellevància l'anomenada "**direcció MAC**": qualsevol tarja de xarxa (cablejada o inalàmbrica, sigui del tipus que sigui) en té una. Aquesta direcció és una "matrícula" única al món que és gravada físicament pel fabricant de la tarja i que serveix, per tant, per identificar físicament aquella tarja de xarxa respecte qualsevol altra,

independentment del sistema operatiu i de la configuració de xarxa que s'utilitzi. Està formada per sis bytes (normalment escrits en hexadecimals i separats entre si per ":"): els tres primers són els mateixos per cada fabricant (s'anomenen genèricament OUI i són assignats per l'organització IEEE) i els altres són únics per la tarja individual. Es pot consultar quina OUI correspon a cada fabricant en aquest formulari online: https://www.wireshark.org/tools/oui-lookup.html

NOTA: En teoria les direccions MAC -al contrari que les direccions IP- són inalterables (és a dir, no es poden canviar i sempre van lligades a un determinat dispositiu concret) però existeixen programes que poden falsificar-la, fent creure a la resta de la xarxa que la tarja en qüestió és una altra diferent de la real.

*Capa d´Internet: Permet el direccionament i l´enrutament dels paquets. És a dir, és on apareix el concepte de **direcció IP,** màscara i porta d'enllaç. Els routers només treballen fins aquí (ignoren la resta de conceptes que apareixen a capes superiors). Cal tenir present que en aquesta capa no hi ha cap tipus de connexió entre els extrems, ni fiabilitats en la comunicació :d´això s´encarrega el nivell superior.

En aquest nivell és on trobem uns paquets especials (els de tipus ICMP), que són, entre altres, els enviats i rebuts pel programa *ping*

*Capa de transport: Aquí apareix el concepte de port. Un **port** és un número que assigna el sistema operatiu a un programa per a què aquest programa pugui rebre i enviar per allà tota la informació que necessiti a un altre port (normalment d'una màquina remota) on estarà, al seu torn, una altra aplicació allà connectada. Els ports permeten mantenir més d'un canal de comunicació en paral.lel de forma totalment independent a la resta de canals establerts i, per tant, aconseguir que la informació transmesa per un canal no afecti en res a cap altre.

Existeixen dos tipus de ports, els TCP i els UDP. La comunicació realitzada entre els primers és fiable (és a dir, els paquets enviats arriben al destí ordenats, sense errors, sense duplicar-se i sense perdre´s) però la realitzada entre els segons no. L'UDP s'utilitza, llavors, en serveis que requereixen velocitat i flexibilitat però no són crítics (com ara un servei d'streaming de vídeo, per exemple).

*Capa d´aplicació: Aquí és on es comuniquen els programes entre sí directament, fent servir el protocol particular que entenguin ells. Normalment, la comunicació entre els programes es realitza d'extrem a extrem, on un dels programes actua com a "client" i l'altre actua com a "servidor". El "client" és qui realitza peticions d'un recurs (per exemple, un navegador seria un client que demana pàgines web) i el "servidor" és qui comparteix aquest recurs (en aquest cas, seria l'ordinador a qui el navegador li ha demanat la pàgina web, el qual la tindrà guardada al seu disc dur). El "servidor" normalment roman permanentment a l'espera ("a l'escolta") per tal de rebre peticions de clients que li demanin un determinat recurs (moment en el qual l'ofereix si efectivament el té disponible) però el client només cal que estigui funcionant en el moment que necessiti demanar (i rebre) el recurs en qüestió.

Depenent del tipus de tasca a realitzar pel servidor, aquest s´haurà de comunicar amb els clients corresponents utilitzant un determinat llenguatge (protocol), de manera que un client quan demani un servei, aquest servidor concret el pugui entendre i respondre´l utilitzant el mateix protocol. És per això que en aquesta capa trobem tants protocols com quasi tipus diferents de programes; alguns dels més habituals, però, són:

HTTP : Protocol usat pels clients web (navegadors) generalment per demanar a servidors web (Apache, Nginx, ...) la descàrrega de recursos web (pàgines, imatges, etc).

HTTPS : Similar al HTTP però afegeix la capa d'encriptació TLS per tal d'aconseguir que la comunicació entre client i servidor es transmeti de forma segura i no pugui ser espiada ni modificada

FTP: Protocol usat per "baixar" i "pujar" fitxers entre un client (el programa usat per l'usuari) i un servidor (que faria de magatzem remot). En desús a favor de WebDAV (una extensió d'HTTP que permet no només descarregar fitxers sinò també pujar-hi al servidor).

SSH: Protocol usat per iniciar sessió a un terminal d'un servidor remot,emprant per això un client local

VNC: Protocol usat per iniciar sessió a l'escriptori d'un servidor remot,emprant per això un client local

SMTP/POP/IMAP : Protocols utilitzats durant l'enviament (SMTP) i recepció (POP o IMAP) d'e-mails

DNS: Protocol emprat pel client per fer una petició DNS i pel servidor per retornar la resposta

DHCP: Protocol emprat pel client per fer una petició DHCP i pel servidor per retornar la resposta

NOTA: Les especificacions oficials d´aquests protocols les estableix l'organització internacional IETF a través d'uns documents anomenats RFC (http://www.ietf.org/rfc.html).

Tots els programes servidors d'un determinat tipus (HTTP, FTP, etc) solen utilitzar per escoltar les peticions un mateix número de port estàndar ja conegut; d'aquesta manera, qualsevol client que sigui del seu tipus ja estarà preprogramat per connectar-s'hi a aquest port per defecte. El repartiment de números de port segons el tipus de servidor que hi hagi "al darrera" està gestionat per l'IANA i es pot consultar aquí http://www.iana.org/assignments/port-numbers (una còpia d'aquesta llista també es troba al fitxer /etc/services) Bàsicament, en aquesta llista s'estableix que hi ha tres tipus de ports:

-Reservats per processos del sistema (1-1023). Això vol dir que són ports importants que només poden ser "oberts" per programes executant-se com a "root". Entre ells, aquí trobem el port 21 (utilitzat pels servidors FTP), el port 22 (utilitzat pels servidors SSH), el port 80 (utilitzat pels servidors HTTP -"web"-), els ports 25, 110 i 143 (utilitzats pels servidors SMTP/POP/IMAP, respectivament), el port 443 (utilitzat pels servidors HTTPS -"web segurs"-), etc. Tots aquests ports són TCP però també estan els UDP...concretament, els servidors DNS escolten al port 53 UDP i els servidors DHCP escolten al port 67 UDP. Tot això es pot canviar a la configuració del programa en qüestió, és clar, però no se sol fer.

-Registrats per aplicacions determinades (1024-49151) . Per exemple, aquí trobem el port 3306 (utilitzat pel servidor MySQL), el port 5900 (utilitzat pels servidors VNC), etc.

-Lliures (49152-65535). Són els que utilitzen els clients, ja que és indiferent quin port fan servir en cada moment (de fet, l'elecció és aleatòria, de manera que, per establir una connexió, una vegada un client pot "agafar" un determinat port que estigui lliure -en realitat, li assigna el sistema operatiu- i un altra vegada pot "agafar" un altre.

Configuració bàsica de la xarxa:

Les tarjes de xarxa en sistemes Linux es poden anomenar de les següents maneres:

lo :	Correspon a la tarja "loopback". Recordem que hem dit que aquesta tarja físicament no existeix (és un "invent" del sistema operatiu) i sol tenir sempre té la IP 127.0.0.1/8. Serveix per establir una connexió amb sí mateixa, de tal forma que podem tenir a la mateixa màquina un programa client que connecti a un programa servidor sense sortir "a fora".
eno1, eno2 .... :	Tarjes Ethernet integrades a la placa base ("on-board")
ens1, ens2 ..... :	Tarjes Ethernet PCI ("slot")
enp2s0, p3p1...:	Tarjes Ethernet que no es poden localitzar d'altra forma degut a limitacions de la BIOS
wlp2s0,... :	Tarjes WiFi

Dins de les màquines virtuals de VirtualBox les tarjes de xarxa agafen sempre un nom concret: la tarja corresponent a la primera pestanya del quadre de configuració de xarxa s'anomenarà "enp0s3" dins del sistema virtualitzat, la segona "enp0s8", la tercera "enp0s9" i la quarta "enp0s10".

Veure la configuració actual

Per veure l'estat i configuració de les tarjes detectades es pot fer servir la comanda **ip address show** (o bé **ip address show dev *nomTarja*** si només es vol obtenir la informació d'una tarja determinada). Concretament ens mostra:

-Les direccions MAC de les tarjes
-El seu estat respectiu (UP, DOWN)
-Les seves direccions IP respectives (i la màscara corresponent)
-Altres dades (com si permet l'enviament "broadcast", si està en mode "promiscu", etc).

NOTA: La comanda *ip address show* es pot escriure de forma més curta així: *ip a s* . Fins i tot, es pot deixar d'escriure el verb *show* (o *s*) perquè és l'acció perfecte (per tant, es pot fer *ip address* o *ip a* i seria el mateix)

Per saber, en canvi, quina és la porta d'enllaç configurada a la nostra màquina, s'ha de fer servir la comanda **ip route show** (o bé **ip route show dev *nomTarja*** o les seves variants *ip route*, *ip r s* o *ip r*). Aquesta comanda ha de mostrar una línia (o més, si la màquina té una porta d'enllaç diferent definida per cadascuna de les seves possibles tarjes) que començarà amb l'expressió "default via" seguida de la direcció IP de precisament la porta d'enllaç establerta (i, a continuació, l'expressió "dev *nomTarja*" per indicar a quina tarja de xarxa s'aplica). Aquesta comanda pot mostrarmés línies, però no ens interessaran gaire...(potser la més curiosa és una que serveix per indicar que no cal cap porta d'enllaç per comunicar-se amb les màquines que precisament pertanyin a la mateixa xarxa a la què pertany la nostra màquina).

Per saber la direcció IP del servidor DNS configurat a la nostra màquina (o les IPs...si n'hi ha més d'una es prova de connectar a la primera i si aquesta falla llavors es prova la segona, i així) es pot consultar l'arxiu **/etc/resolv.conf** (concretament, les línies que comencen per la paraula *nameserver*). El contingut d'aquest arxiu sol ser gestionat a la vegada per diferents programes automàticament (com ara pot ser el client dhclient, l'aplicació NetworkManager, el servei "networking", el servei "systemd-networkd/resolved", etc). No es recomana modificar-lo manualment ja que els canvis realitzats a mà podrien "matxacar-se" sense avisar en qualsevol

moment per qualsevol d'aquests programes. En aquest sentit, aquests programes (dhclient, NetworkManager, "networking", "systemd-networkd/resolved, etc) guarden els servidors DNS que usen dins dels seus propis arxius de configuració i els manipulen allà de forma autònoma (per exemple NetworkManager usa /var/run/NetworkManager/resolv.conf, "systemd-resolved" usa /run/systemd/resolve/resolv.conf, "networking" usa la línia dns-nameservers dins de /etc/network/interfaces, etc) però a més sempre vinculen en forma d'enllaç simbòlic el seu arxiu propi respectiu a l'arxiu comú /etc/resolv.conf per a què els programes que facin servir aquest arxiu comú no tinguin problemes en trobar els servidors DNS. Als exercicis es veuran casos pràctics de com gestionar tot això.

Canviar la configuració de forma temporal

*Per assignar una IP/màscara concreta a una tarja: **ip address add *v.x.y.z/n* dev *nomTarja***

*Per esborrar una IP/màscara concreta a una tarja: **ip address del *v.x.y.z/n* dev *nomTarja***

NOTA: També es pot fer **ip [-4|-6] address flush dev *nomTarja*** si el que es vol és esborrar de cop qualssevol de les eventuals diferents direccions IP que pugui tenir la tarja indicada

*Per assignar la porta d'enllaç concreta a una tarja: **ip route add default via *v.x.y.z* dev *nomTarja*** . Abans, però, s'hauria d'esborrar la que hi havia assignada abans (si no es fa dóna error), així: **ip route del default dev *nomTarja*** .

NOTA: També es pot escriure **ip route add 0.0.0.0/0 via v.x.y.z dev nomTarja.** És equivalent.
NOTA: De forma alternativa, en comptes de fer *ip route del ...* i després *ip route add ...*, el canvi de porta d'enllaç per defecte es podria fer directament en un sol pas, així: **ip route change default via v.x.y.z dev nomTarja**
NOTA: També es pot indicar que es vol fer servir una determinada porta d'enllaç només per arribar a una xarxa-destí concreta. En aquest cas, llavors, no estaríem parlant de porta d'enllaç "per defecte" sinò d'una porta d'enllaç "específica". La porta d'enllaç "per defecte" seria usada llavors que el sistema hagués comprovat que el destí desitjat no forma part del conjunt de destins indicats a portes d'enllaç específiques. Per crear una porta d'enllaç específica cal executar la comanda **ip route add ip.Xarxa.Desti/Mascara via v.x.y.z dev nomTarja**
Es pot afegir a més un darrer paràmetre **metric nº**, que indica la preferència de la ruta en el cas de què hi haguessin vàries que portessin al mateix destí (a mode de "backup"): un nº menor indica una major preferència
NOTA: Un cop assignada una direcció IP a una tarja, el sistema calcula automàticament la seva direcció IP de xarxa corresponent i genera una ruta a ella (és per això que és necessari indicar la màscara en *ip address add...*)
Per exemple, si s'assigna la IP 203.0.113.25/24 a la tarja enp0s3, es crearà automàticament una ruta a la xarxa 203.0.113.0/24 directa, de manera que el sistema sabrà que per comunicar-se amb hosts d'aquesta xarxa no necessitarà cap porta d'enllaç intermediària sinó que ho podrà fer directament.

*Per activar/desactivar una tarja: **ip link set {up|down} dev *nomTarja***

Canviar la configuració de forma permanent

Totes les comandes anteriors, no obstant, només "funcionen" mentre la màquina es manté encesa: si s'apaga llavors les direccions IP/màscares i portes d'enllaç configurades amb les comandes "ip" anteriors es perden i cal, doncs, tornar-les a executar un altre cop al següent inici. Per tal de què la configuració desitjada de IP/màscara i porta d'enllaç (i servidor DNS també, gestionat amb algun dels programes comentats en paràgrafs anteriors) per una determinada tarja de xarxa es mantingui de forma permanent a cada reinici de la màquina, cal escriure els valors adients en un determinat arxiu. En sistemes Debian/Ubuntu, aquest arxiu s'anomena /etc/network/interfaces i ha de tenir un aspecte similar al següent (les línies que comencen per # són comentaris; les tabulacions són opcionals):

#Les línies "auto" serveixen per activar la tarja en qüestió (en aquest cas, la tarja "lo")
auto lo
#La línia següent indica que la tarja "lo" és de tipus "loopback" (i que, per tant, tindrà la IP 127.0.0.1)
iface lo inet loopback
#En el mateix arxiu es poden configurar totes les tarjes que es vulguin: la següent s'anomena enp3s0
auto enp3s0
#La paraula "static" indica que els valors d'IP, màscara, etc són fixes a cada reinici
iface enp3s0 inet static
#A continuació s'indiquen els valors d'IP, màscara, porta d'enllaç i servidors DNS que es volen assignar
address v.x.y.z
netmask w.w.w.w
gateway v.x.y.z
dns-nameservers v.x.y.z v.x.y.z

Establir una configuració dinàmica

En les configuracions anteriors, tant la temporal com la permanent, s'estableix una direcció IP/màscara + porta d'enllaç concreta, decidida per nosaltres. Aquest mètode pot ser útil per poques màquines, però en una xarxa amb moltes d'elles pot arribar a ser força farragós, a més de que fàcilment es poden cometre errors (IPs duplicades, IP no assignades). Un altre mètode per establir aquestes dades és el mètode "dinàmic", en el qual la màquina en qüestió no té assignada de forma fixa cap IP/màscara + porta d'enllaç + servidor DNS sinò que aquestes dades les pregunta a la xarxa: allà hi haurà d'haver escoltant un ordinador executant un software especial anomenat "servidor DHCP", el qual serveix precisament per atendre aquestes peticions de "dades de xarxa" i assignar-les a qui les demani. D'aquesta manera, es té una gestió centralitzada del repartiment de direccions IP/màscara + porta d'enllaç + servidors DNS sense que calgui realitzar cap configuració específica a les màquines clients. Això sí, és clar: primer caldrà haver instal.lat i configurat convenientment a la nostra xarxa aquest software "servidor DHCP" (un exemple és el paquet "isc-dhcp-server"), tasca que no veurem (presuposarem que això ja està fet).

NOTA: Segons com es configuri el servidor DHCP, aquest podrà assignar més o menys quantitat d'IPs, assignarà sempre la mateixa IP a la mateixa màquina (identificada per la MAC de la seva tarja), etc...però això ja està fora del nostre control si no som l'administrador de la xarxa.

La manera de demanar les dades de xarxa a algun servidor DHCP que estigui present a la nostra xarxa pot realitzar-se de forma automàtica cada cop que la nostra màquina arrenqui (de manera que nosaltres no haguem de fer res i ja tinguem, si tot va bé, aquestes dades ja assignades un cop iniciem sessió) o també de forma manual cada cop que volguem executant la comanda *dhclient*. Concretament, la primera forma s'activa simplement escrivint les següents línies a l'arxiu /etc/network/interfaces:

auto enp3s0
iface enp3s0 inet dhcp

D'altra banda, la comanda *dhclient* funciona de la següent manera:

dhclient *nomTarja* Demana -per a la tarja indicada- les dades de xarxa (IP, màscara, porta d'enllaç, servidor DNS, etc) a algun servidor DHCP que estigui escoltant a la LAN de la nostra màquina

-v Mostra per pantalla tot el procés de petició i resposta (útil per veure si va)

-r Esborra totes les dades de xarxa que pugui tenir actualment la tarja indicada

Comandes bàsiques de xarxa:

ping ip.oNom.Maq.Remota — Comprova si la màquina remota indicada respon. Serveix, per tant, per saber si hi ha connexió de xarxa amb aquella màquina (si no, podria ser degut a qualsevol causa: cable mal endollat o trencat, màquina remota apagada, etc). En aquest sentit, són interessants les dades estadístiques que apareixen al final (paquets enviats, rebuts, perduts, etc) i el temps que han trigat en enviar-se aquests paquets de prova (i rebre's la resposta) -i així comprovar la saturació del medi.

- *-n* No resol noms (és a dir, no fa la consulta prèvia al servidor DNS del sistema). Per tant, només fa que funcioni indicant direccions IP
- *-c nº* Número de paquets de prova que s'enviaran (si no s'indica, són infinits i cal aturar l'enviament pulsant CTRL+C)
- *-i nº* Número de segons que s'espera per enviar el següent paquet
- *-f* Mode "flood". Envia paquets a la màxima velocitat possible, mostrant un punt per cada paquet enviat i esborrant-lo per cada resposta rebuda: per tant, per anar bé caldría que només es veiés un punt i anés desapareixent: si es veuen molts punts és que hi ha pèrdua de paquets. Cal ser root per a què funcioni
- *-I eno1* Indica la tarja de xarxa per la qual s'enviaran els paquets (per si la màquina tingués més d'una)

mtr ip.oNom.Maq.Remota — Serveix per conèixer el camí seguit per un paquet des de la màquina origen fins l'indicada, mostrant la IP (o nom) de tots els routers intermitjos a través dels quals va passant. També mostra estadístiques dels temps emprat en cada paquet, el millor temps, el pitjor, els paquets perduts, etc

- *-n* No resol noms (és a dir, no fa la consulta prèvia al servidor DNS del sistema).
- *-c nº* Número de paquets de prova que s'enviaran (si no s'indica, són infinits i cal aturar l'enviament pulsant CTRL+C)
- *-i nº* Número de segons que s'espera per enviar el següent paquet

ss — Mostra dades sobre les connexions existents (o que poden existir) a la nostra màquina. Concretament, mostra l'estat de la conexió (els més habituals són ESTABLISHED i LISTEN -aquest últim indica que el port està obert però sense connexió-... altres estats sovint són temporals i acaben derivant en una connexió establerta o bé desapareixent), mostra la IP i el port local utilitzats per establir la connexió (o per escoltar, segons) i la IP i port remot on la corresponent IP+port local estan connectats .

NOTA: Les columnes "Recv-Q" i "Send-Q" mostren la quantitat de bytes que estan actualment al buffer temporal de memòria que gestiona el kernel per tal de regular la recepció i enviament de dades, respectivament.El normal es que valguin 0, indicant així que no hi ha cap dada d'entrada que s'estigui esperant a ser processada pel sistema ni cap dada de sortida que s'estigui esperant a efectivament sortir, respectivament

- *-t* Mostra només les connexions TCP actuals
- *-u* Mostra només les connexions UDP actuals
- *-n* No resol noms (és a dir: mostra IPs i ports en format numèric en comptes de amb noms)
- *-a* (Combinat amb -t i/o -u): Mostra, a més de les connexions actuals, els ports a l'escolta

-l	(Combinat amb -t i/o -u): Mostra només els ports a l'escolta (les connexions actuals no)
-p	(Combinat amb -t i/o -u): Mostra 1 columna més: l'executable "al darrera" de cada port local
-s	Mostra un resum amb estadístiques

ncat ip.oNom.Maq.Remota nºport	Client Netcat que ve dins del paquet "nmap": realitza una connexió (TCP) a la màquina i port indicat. Es pot afegir el paràmetre -v (mode verbós) i -n (no resol noms), entre altres.
-v	Mode verbós (-vv és més verbós i -vvv més encara)

ncat -l -k -p nº	Servidor Netcat: posa a l'escolta el port (TCP) indicat. El paràmetre -l serveix per "obrir" el port, el paràmetre -p serveix per indicar el número de port a obrir i el paràmetre -k permet que s'hi puguin connectar més d'un client a la vegada.
-e /ruta/comanda	Tot el que es rebi de la xarxa serà passat a la comanda indicada, la sortida de la qual serà retornada al client. Si la comanda indicada fos /bin/bash, l'entrada s'entendrà com una comanda a executar (i la sortida serà la sortida de la comanda executada).

Exemples Ncat

*__Chat__
Servidor: *ncat -l -p 5588* <---> Cliente: *ncat ipServidor 5588*
El servidor se pone a escuchar en el puerto 5588 (por defecto siempre es TCP), con lo que todo lo que le llegue de la red -es decir, del cliente-lo pasará a la stdout (pantalla), y todo lo que escriba por stdin (teclado) pasará a la red -es decir, hacia el cliente-. Lo mismo ocurre en el otro lado de la comunicación. Si se añade el parámetro -k al servidor, múltiples clientes podrán enviar mensajes al servidor y este, lo que envíe, lo enviará a todos sin discriminación

*__Envío de un archivo__
Servidor: *ncat -l -p 5555 < archivo* <---> Cliente: *ncat ipServidor 5555 > archivo*
Muy similar a lo anterior: el servidor se pone a escuchar en el puerto 5555, pero en vez de responder por teclado a la stdin, la entrada proviene de un archivo, el cual esperará latente a que cuando se establezca una comunicación por ese puerto, su contenido viaje bit a bit por la red hacia el cliente, el cual lo recibirá y lo guardará en forma de archivo otra vez. Lo malo es que tal como se ha hecho, no se sabe cuándo se ha acabado la transferencia: hay que esperar un tiempo prudencial y entonces hacer Ctrl+C.

*__Reproducción de audio en streaming__
Servidor: *ncat -l -p 5858 <archivo.mp3* <--->Cliente: *ncat ipServidor 5858 | mpg123 -*
El ejemplo es idéntico al anterior, teniendo un archivo en este caso de audio. La única diferencia es que en el cliente, el archivo no se redirecciona para grabarlo en disco sino que se entuba a un reproductor de audio por consola, como mpg123 (el guión del final es para indicarle que el fichero o lista de reproducción le proviene de la tubería).

*__Clonación de discos por red__
Servidor: *ncat -l -p 5678 | dd of=a.iso.gz* <---->Cliente: *dd if=/dev/sda | gzip -c | ncat ipServidor 5678*
El ejemplo es parecido al anterior: primero en el cliente se comprime bit a bit el contenido del disco "sda" y se le envía ya comprimido al servidor, el cual recibe este contenido binario y lo almacena en un archivo, bit a bit too.

nmap -sn { ipInici-ipFinal [altraIP ...] | ipAmbAsterisks } Mostra quins ordinadors estan presents a la xarxa. Existeixen molts altres paràmetres d'escaneig (-sU, -sX, -sF, etc) que fan servir diferents tècniques més o - ràpides/sigiloses/precises, però no les veurem.

-v Mode verbós (-vv és més verbós i -bb més encara)

-n No resol noms

nmap -p nº,nº-nº ipOrdinador Mostra quins ports (del rang indicat) té oberts un ordinador concret. Aquí també es poden fer servir diferents tècniques però tampoc aprofundirem

-O Mostra el sistema operatiu de l'ordinador i els programes "al darrera" dels ports oberts. Es pot combinar amb el paràmetre -sV, el qual mostra també les versions. El paràmetre -A és la combinació dels dos.

El nom de la màquina que veiem en el prompt no és un nom DNS, sinò que ve especificat a l'arxiu /etc/hostname (i per tant, pot ser el mateix a múltiples ordinadors de la xarxa). Per gestionar aquests noms es pot fer servir la comanda **hostnamectl** (sense paràmetres mostra aquest nom i altres valors relacionats; amb el paràmetre *set-hostname nouNom* estableix un nou nom). En tot cas, aquest nom és local.

Si queremos tener una relación entre nombres de máquina y direcciones IP para varias máquina de nuestra red pero no queremos (o podemos) poner en marcha un servidor DNS propio, una alternativa es modificar el archivo /etc/hosts en cada una de las màquinas que queramos nombrar. Este archivo ha de contener, precisamente, la lista de las IPs del resto de ordenadores de la red (una por línea), cada una de ellas (seguidas en su misma línea) pr el nombre (o nombres, separados por espacios) que queremos que nuestra máquina interprete como equivalente. Por defecto, este archivo se consultará siempre antes de preguntar a un servidor DNS*, lo que puede facilitar la realización de censuras.

*Esto es así siempre y cuando la línea "hosts: ..." que hay dentro del archivo /etc/nsswitch.conf contenga la palabra "files" antes (es decir, a la izquierda) de la palabra "dns".

nslookup nomDNS [ip.serv.DNS] Client DNS que pregunta al servidor indicat o, si no s'indica cap, al que estigui configurat a /etc/resolv.conf. Normalment, a més de retornar la IP (o IPs equivalents) associades al nom indicat, també mostra els "àlies" que té aquest nom

NOTA: Un altre client similar és la comanda *host nomDNS [ip.serv.DNS]*
NOTA: Un altre client més complet és la comanda *dig [@ip.serv.DNS] nomDNS*. O *drill*
NOTA: Un altre client però només compatible amb *systemd-resolved* és *systemd-resolve*

whois dominiDNS Consulta els servidors WHOIS administrats per la IANA per esbrinar les dades administratives de l'empresa que ha llogat el domini indicat

wget https://url/dun/fitxer Descarrega al disc dur el fitxer indicat

-c Continua la descàrrega (si anteriorment va fallar) des d'allà on es va interrompre

-O nom Indica el nom que tindrà el fitxer un cop descarregat

-r Realitza una descàrrega recursiva si la URL indicada és la d'una carpeta en comptes de la d'un fitxer. Combinat amb el paràmetre *-l nº* serveix per indicar fins a quin nivell (1=una subcarpeta, 2= dues subcarpetes) es vol descarregar...si no s'indica s'entén "infinit"

-N Descarrega només els arxius més nous que els locals

-A "ext1","ext2",... Descarrega només els arxius que trobi amb l'extensió indicada
El paràmetre contrari (descarrega tot excepte els arxius indicats) és -R

--no-parent	No descarrega contingut anterior a la URL indicada
-nd	Tot o descarrega a la mateixa carpeta local (sense respectar, doncs, la jerarquia de carpetes del lloc remot)
-k	Un cop feta la descàrrega, transforma els enllaços per tal de què tot el contingut es pugui visitar offline (canvia les rutes absolutes per relatives i als recursos no descarregats els referencia amb la URL completa)

curl https://url/dun/fitxer Descarrega al disc dur el fitxer indicat

-o nom	Indica el nom que tindrà el fitxer un cop descarregat
-s	Mode "silenciós" (no mostra les estadístiques de descàrrega)
-L	Si el servidor web retorna un codi de redirecció (3xx), el segueix automàticament
-I	No descarrega el fitxer: només mostra la capçalera de resposta HTTP del servidor
-H capçalera=valor	Realitza una petició indicant un valor concret per la capçalera HTTP de client indicada

lynx https://url/duna/pagina Navegador en mode text. N'hi ha d'altres (elinks, w3m)