# Comandes bàsiques de xarxa (Nivell 4)

*ss* Mostra dades sobre les connexions existents (o que poden existir) a la nostra màquina. Concretament, mostra l'estat de la connexió (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 esperant a 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 lloc de amb noms)
- *-a* (Combinat amb *-t* i/o *-u*): Mostra, a més de les connexions actuals, els ports escoltant
- *-l* (Combinat amb *-t* i/o *-u*): Mostra només els ports escoltant (les connexions actuals no)
- *-p* (Combinat amb *-t* i/o *-u*): Mostra 1 columna més: l'executable "al darrera" de cada port local. Per funcionar necessita ser executat com a usuari administrador.
- *-s* Mostra un resum amb estadístiques

---

Client Ncat

*ncat ip.oNom.Maq.Remota nºport* Client Netcat que ve dins del paquet "ncat" (a Ubuntu) i "nmap-ncat" (a Fedora). Realitza una connexió TCP a l'adreça IP i port indicat.

- *-v* Mode verbós (*-vv* és més verbós i *-vvv* més encara)
- *-n* No resol noms
- *-w nº* Indica el número de segons que el client s'esperarà a intentar establir una connexió abans de deixar-ho córrer
- *-i nº* Indica el número de segons que el client s'esperarà a rebre dades de l'altre extrem abans de tancar la connexió (aquest paràmetre també és vàlid per especificar-ho en el servidor).

Servidor Ncat

*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 nº 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, per tant, com una comanda a executar (i la sortida serà la sortida de la comanda executada).
- *--broker* Fa d'enllaç de comunicacions entre tots els clients entre sí per tal d'implementar una xarxa "tots els clients amb tots els clients", però sense ser-ne visible per ells
- *-u* Indica que el port indicat és de tipus UDP. Si s'usa, aquest mateix paràmetre s'haurà d'escriure també en el client.

Altres paràmetres interessants de *ncat* són *--send-only/-recv-only*, *--allow/--allowfile*, *--deny/--denyfile* o *--max-conns* (consulteu el manual per conèixer els seus usos)

Exemples Ncat

***Chat**
Servidor: *ncat -l -p 5588* <---> Client: *ncat ipServidor 5588*
El servidor es posa a escoltar en el port 5588 (per defecte sempre és TCP), de manera que tot el que li arribi de la xarxa (és a dir, del client remot) ho passarà a la *stdout* (pantalla), i tot el que escrigui per *stdin* (teclat) passarà a la xarxa (és a dir, cap al client). El mateix passa a l'altra banda de la comunicació. Si s'afegeix el paràmetre *-k* a servidor, múltiples clients podran enviar missatges a el servidor i aquest, el que enviï, el trametrà a tots sense discriminació

***Enviament d'un arxiu**
Servidor: *ncat -l -p 5555 < arxiu* <---> Client: *ncat ipServidor 5555 > arxiu* (descàrrega)
Servidor: *ncat -l -p 5555 > arxiu* <---> Client: *ncat ipServidor 5555 < arxiu* (pujada)
Molt similar a l'anterior: en el primer cas el servidor es posa a escoltar en el port 5555, però en comptes de respondre per teclat a *stdin*, l'entrada prové d'un arxiu, el qual esperarà latent al fet que quan s'estableixi una comunicació per aquest port, el seu contingut viatgi bit a bit per la xarxa cap al client, el qual el rebrà i el guardarà en forma d'arxiu una altra vegada. Desgraciadament, tal com s'ha fet, no se sap quan s'ha acabat la transferència: cal esperar un temps prudencial i llavors fer Ctrl + C. En el segon cas és al revés, el servidor es posa en marxa escoltant al primer client que li envïi un fitxer, el qual rebrà i guardarà.

***Reproducció d'àudio en streaming**
Servidor: *ncat -l -p 5858 <arxiu.mp3* <--->Client: *ncat ipServidor 5858 | mpg123 -*
L'exemple és idèntic a l'anterior, en aquest cas amb un arxiu d'àudio. L'única diferència és que en el client l'arxiu no es redirecciona per gravar-ho en disc sinó que s'entuba a un reproductor d'àudio per consola, com és *mpg123* (el guió del final és per indicar-li que el fitxer o llista de reproducció li prové de la canonada).

***Clonació de discos per xarxa**
Servidor: *ncat -l -p 5678 | dd of=arxiu.iso.gz* <---->Client: *dd if=/dev/sda | gzip -c | ncat ipServidor 5678*
L'exemple és semblant a l'anterior: primer al client es comprimeix bit a bit el contingut del disc "sda" i se li envia ja comprimit al servidor, el qual rep aquest contingut binari i l'emmagatzema en un arxiu, bit a bit també

NOTA: La comanda *ncat* que és una millora del programa "netcat" clàssic. Entre altres avantatges, *ncat* té la capacitat de treballar amb IPv6, utilitzar proxys o realitzar connexions segures via TLS, coses que el "netcat" clàssic no pot. A l'Ubuntu encara s`ofereix, però, el "netcat" clàssic. De fet, hi ha disponibles dos paquets que representen sengles variants del programa "Netcat" clàssic (*netcat-openbsd* i *netcat-traditional*). Per defecte està instal.lat el primer (encara que no el farem servir). La diferència més important entre aquests dos paquets clàssics és que en l'"openbsd" no existeixen els paràmetres *-c* ni *-e* (que sí hi són al "traditional"). Un dubte que podem tenir és que si volguéssim tenir aquest darrer instal.lat també, ¿quin dels dos netcat s'executaria llavors quan escrivim “nc” a la línia de comandes? La resposta és que, en realitat, en aquest cas “nc” seria un enllaç a l'arxiu "/etc/alternatives/nc", el qual al seu torn és un enllaç al binari exacte que es vol executar ("/usr/bin/nc.openbsd" ó "/usr/bin/nc.traditional"). Per gestionar aquest esquema d'enllaços a executables alternatius a sistemes Debian existeix la comanda *update-alternatives*, que se sol fer servir per gestionar enllaços amb un nom genèric (“browser”,”editor”,”nc”...) -anomenats “links”- que apunten als altres ubicats centralitzadament a "/etc/alternatives" -anomenats “names”, el quals apunten al binari concret a executar -anomenat “path”- Té les següents opcions, evidents:

*update-alternatives --install link name path*
*update-alternatives --remove name path*
*update-alternatives --set name path*
*update-alternatives --display name*

Nmap: Escaneig de xarxes

*nmap -sn { ipInici-ipFinal [altraIP ...] | ipXarxa/mask | ipAmbAsterisks }* Mostra quins ordinadors estan presents a la xarxa/rang indicat.

Per indicar el rang a escanejar, tal com es veu, es poden escriure diferents alternatives (a combinar):

-Una IP de host individual o diferents IPs de hosts individuals separades per espais
-Un rang d'IPs indicat per guions (p. ex: 192.168.1.3-5 ó 10.0.0-255.1-254, etc)
-Un conjunt d'IPs indicat per comes (p. ex: 192.168.1.3,5 ó 10.0.0,1,4.1, etc)
-Una IP de classe C escrita amb el comodí * (p. ex: 192.168.1.*)
-Una IP de xarxa amb la seva màscara corresponent (p. ex: 192.168.1.0/24)
-Igualment, es poden indicar hostnames
-El paràmetre *--exclude* o (*--excludefile)* per indicar, amb mateixes normes, subrangs exclosos

El paràmetre *-sn* permet veure si els ordinadors indicats estan presents a la xarxa però sense fer cap escaneig de ports. Això fa que l'escaneig per detectar una simple presència de màquines sigui més ràpid. Concretament, aquest paràmetre fa que Nmap envii dos paquets TCP SYN als ports 80 i 443 de cada destí,

NOTA: La idea de detectar un destí concret enviant-li paquets SYN és bàsicament que si se n'obté resposta (bé sigui via paquet RST-ACK perquè el port demanat estigui tancat o bé via paquet SYN-ACK si està obert -llavors Nmap finalitzaria l'escaneig amb un paquet RST-ACK-), el destí es trobarà encès, però si no se n'obté cap resposta passat un determinat "timeout", doncs es conclourà que el destí es troba apagat o no existeix.

NOTA: Si s'executa Nmap amb el mateix paràmetre *-sn* però com a "root", llavors els paquets TCP SYN anteriors se substitueixen per un paquet ARP "broadcast". Una altra opció seria fer l'escaneig mitjançant paquets ICMP però aquests poden estar filtrats i és per això que no es fan servir; no obstant, si s'executa Nmap amb el mateix paràmetre *-sn*, com a "root" i, a més, afegint-hi a més el paràmetre *--send-ip*, als paquets TCP SYN descrits al paràgraf anterior llavors sí s'afegirà l'enviament a cada destí de dos paquets més, tots dos de tipus ICMP (en concret un de tipus "echo-request" i l'altre de tipus "timestamp").

Si es vol, no obstant, canviar el tipus de paquets utilitzats a l'hora de detectar màquines a la xarxa per altres de diferents (la raó de fer-ho és que, depenent de les circumstàncies de la xarxa concreta a escanejar, algun d'aquests paràmetres podrien obtenir resultats més precisos), es pot afegir al paràmetre *-sn* algun dels següents paràmetres opcionals llistats a la taula següent:

| | |
|---|---|
| ***-PS nº,nº-nº*** | Envia paquets TCP SYN als ports indicats i n'espera resposta (de tipus SYN-ACK o RST-ACK segons si el port està obert o tancat, respectivament). Podem veure, doncs, que *-sn* és equivalent a *-PS80,443* |
| ***-PA nº,nº-nº*** | Envia paquets TCP ACK als ports indicats i n'espera resposta (de tipus RST-ACK sempre). Només funciona si s'executa com a "root". |
| ***-PU nº,nº-nº*** | Envia paquets UDP als ports indicats i n'espera resposta. Si el port en qüestió estigués tancat (el que es vol), es rep un paquet ICMP de tipus "Port unreachable" |
| ***-PY nº,nº-nº*** | Envia paquets SCTP als ports indicats i n'espera resposta (de tipus "Init-ACK" o "Abort" segons si el port està obert o tancat, respectivament) |
| ***-PE*** | Envia un paquet ICMP "echo-request" (un "ping") i n'espera resposta. Cal ser "root" |
| ***-PP*** | Envia un paquet ICMP "timestamp" i n'espera resposta |
| ***-PM*** | Envia un paquet ICMP "netmask-request" i n'espera resposta |
| ***-PR*** | Envia un paquet ARP. Només funciona si s'executa com a "root", Si és així, però, aquest paràmetre és implícit a la resta de paràmetres anteriors si Nmap detecta que l'escaneig es fa a màquines de la nostra xarxa local, així que en aquest cas no se sol fer escriure explícitament. De fet, moltes vegades és al revés: el que es fa és afegir el paràmetre *–send-ip* per no realitzar l'enviament del paquet ARP i llavors així obligar a fer l'enviament ICMP/TCP/UDP per detectar el destí de la nostra xarxa local d'aquesta manera i no pas amb ARP (amb destins fora de la nostra xarxa no cal indicar *--send-ip* perquè no s'usa el paràmetre *-PR* implícitament mai) |

Nmap: Escaneig de ports

*nmap -Pn -p nº,nº,nº-nº ipOrdinador* : Comprova quins ports (dels indicats amb el paràmetre *-p*) estan oberts a l'ordinador "objectiu". Si no s'indica cap paràmetre *-p*, l'Nmap escanejarà els 1000 ports més comuns.

NOTA: Els ports més comuns es troben llistats al fitxer "**/usr/share/nmap/nmap-services**" (cal observar els que tinguin un major valor a la columna "open frequency"). Amb el paràmetre *-F* s'escanejaran els 100 més comuns. Altres paràmetres interessants en aquest sentit són *--top-ports x* i *--exclude-ports nº,nº-nº*

Si ja sabem que la "víctima" està accessible a la xarxa (perquè, per exemple, ho hem vist amb l'escaneig de xarxa previ) i només ens interessa fer l'escaneig de ports directament sense haver de fer cap comprovació prèvia podem estalviar-nos aquest "pas de descoberta" innecessari amb el paràmetre *-Pn*

NOTA: En realitat, es podrien fer totes dues coses d'un sol cop (escaneig de xarxes i de ports) escrivint una comanda similar a *nmap -p nº,nº,nº-nº { ipInici-ipFinal [altraIP ...] | ipAmbAsterisks | ipXarxa }*

Un altre paràmetre que se sol afegir quan es fan escanejos de ports és el paràmetre *-A* , el qual és, en realitat, la combinació de varis paràmetres en un: el *-O* (que mostra el nom del sistema operatiu de l'ordinador; requereix privilegis d'administrador), el *-sV* (que mostra el nom dels programes que hi ha escoltant "al darrera" dels ports oberts i les versions respectives), el *-sC* (que en parlarem més endavant) i fa un "traceroute".

D'altra banda, existeixen molts altres paràmetres (*-sS, -sT, -sA, -sW, -sN, -sF, -sX, -sM, -sU, -sY, -sZ,* ...) que permeten especificar la tècnica concreta a fer servir per esbrinar si un port està obert o no: algunes tècniques són més ràpides però a canvi són menys sigiloses i/o precises, o viceversa El tipus d'escaneig de ports per defecte que Nmap fa servir si no s'indica cap es correspon al que s'indicaria amb el paràmetre *-sS* si s'executa com a "root" o *-sT* si no. Molt resumides, les tècniques usades són:

NOTA: Si els escanejos següents no reben cap resposta passat un determinat *timeout*, el port s'identificarà com a "filtered", ja que no es pot establir amb claredat si està obert o tancat, ja que podria ser que algun dispositiu intermig (un tallafocs, normalment) hagués eliminat la petició o resposta justament per no donar informació. També es pot obtenir el valor "filtered" si, en el cas de l'escaneig -sS, per exemple, s'obté com a resposta un paquet ICMP de tipus 3 amb codis 1,2,3,9,10 o 13

| | |
|---|---|
| ***-sS*** | Envia un paquet TCP SYN al/s port/s indicat/s. Es dedueix si està tancat o obert segons si es rep una resposta RST-ACK o SYN-ACK (tancant-la llavors amb un RST-ACK per no completar el 3-way handshake), respectivament. |
| ***-sT*** | Realitza un 3-way handshake TCP complet (SYN,SYN-ACK,ACK) al/s port/s indicat/s. Menys eficient que l'anterior però, a diferència d'aquest, es pot realitzar sense ser "root". |
| ***-sA*** | Envia un paquet TCP ACK al/s port/s indicat/s. Si es rep un paquet RST vol dir que el port en qüestió no es troba "filtrat". No serveix, però, per saber si està obert o tancat. |
| ***-sW*** | Similar a l'anterior però inspeccionant el valor del camp "Window" del paquet RST rebut en pot deduir si està obert o tancat. Depèn, però, de la implementació concreta de la pila TCP que tingui la màquina remota, així que cal completar el resultat amb altres dades. |
| ***-sF*** | Envia un paquet TCP FIN al/s port/s indicat/s. Si es rep un paquet RST vol dir que el port en qüestió està tancat i si no es rep res voldria dir que està obert |
| ***-sN*** | Similar a l'anterior però enviant un paquet TCP "Null" (és a dir, amb tots els seus "flags" a 0) |
| ***-sX*** | Similar a l'anterior però enviant un paquet TCP "Xmas" (és a dir, amb els seus "flags" FIN, URG i PSH a 1) |
| ***-sM*** | Similar a l'anterior però enviant un paquet TCP FIN-ACK |
| ***-sU*** | Envia un paquet UDP al/s port/s indicat/s. Si es rep una resposta ICMP de tipus "Port unreachable", el port estarà tancat. Si no es rep res, no se podrà saber si està filtrat o obert. En qualsevol cas, aquest escaneig és molt lent perquè UDP és un protocol no confiable. D'altra banda, en el cas de voler-ho combinar amb algun dels altres paràmetres (que impliquen paquets TCP), a l'hora d'indicar el número de port es pot precedir amb la marca "U:" (si és UDP) o "T:" (si és TCP) per distingir-los. Per exemple: *nmap -sU -sS -p U:137,53,T:139 ...* |

Altres paràmetres interessants que es poden indicar, en qualsevol tipus d'escaneig (de xarxes o de ports) són:

| | |
|---|---|
| *-v* | Mode verbós (*-vv* és més verbós). També està *-d* (mode "debug") |
| *-n* | No resol noms. També està el paràmetre *–dns-servers x.x.x.x,y.y.y.y* , que permet indicar altres servidors DNS a usar per resoldre noms diferents dels predefinits al sistema. En aquest sentit, és interessant el paràmetre *-sL ipXarxa/mask* per fer una consulta DNS inversa per tots els ordinadors de la xarxa indicada i així descobrir els seus noms associats a les seves IPs |
| *-e nomTarja* | Fa servir explícitament la tarja de xarxa indicada per l'escaneig |
| *-T{0-5}* | Estableix retard entre paquet i el següent, per fer l´escaneig més o menys sigilós. El valors admesos (de més a menys lents) són: "paranoid" (0), "sneaky" (1), "polite" (2), "normal" -per defecte- (3), "aggressive" (4), "insane" (5). |
| *-iL nomFitxer.txt* | Indica el fitxer des d'on s'agafaran les IPs i noms dels rangs o ordinadors a escanejar (en lloc de pel terminal); si ha vàries poden estar separades per espais en blanc, tabuladors o salts de línia |
| *-oN nomFitxer.txt* | El resultat de l'escaneig el guarda en un fitxer. El paràmetre *-oN* treu la sortida "normal", però també es pot fer servir *-oX* per a què la sortida sigui en XML o *-oG* per a què sigui fàcilment processable per Grep, entre altres. La combinació dels 3 formats es pot fer amb *-oA* |
| *--packet-trace* | Mostra la traça de tots els paquets enviats pel Nmap en realitzar la seva feina (va bé per estudiar) |
| *--host-timeout <n>* | Estableix un temps (del tipus "3s", "2m", "7h", etc) màxim després del qual, si no s'ha finalitzat l'escaneig abans, aquest s'aturarà. |
| *--reason* | Mostra el motiu de com Nmap ha esbrinat que cada port està en l'estat en que està (tancat, obert, filtrat) |

---

| | |
|---|---|
| *nping ... ipOrdinador* | Eina, proporcionada pel paquet "nmap", que serveix per generar paquets de tipus ARP i de tipus IP (és a dir, ICMP o UDP o TCP) totalment personalitzats (indicant els valors desitjats pels camps que escollim) i enviar-los al destí indicat (el qual pot escriure's fent servir les mateixes regles que amb l'Nmap: una IP de host, una Ip de xarxa, un rang d'IPs, etc). El que mostra aquesta comanda a pantalla son els valors estadístics típics de la comanda *ping* estàndar (RTT min/max/avg, % paquets perduts...) però, com a novetat, també mostra informació no només del paquet enviat sinó també del paquet rebut en contestació (si n'hi ha). |

Les característiques concretes del paquet creat i enviat s'indicaran al lloc dels punts suspensius mitjançant els paràmetres adients, els més rellevants dels quals són:

| | | |
|---|---|---|
| *-c nº* | | Indica quants paquets totals es volen enviar |
| *--rate nº* | | Indica quants paquets per segon es volen enviar. Una alternativa a aquest paràmetre seria *--delay nº* que indica el nombre de segons entre paquet i paquet (es pot indicar el sufixe *ms*) |
| *--arp* | | Indica que es vol enviar paquet/s ARP, on ... |
| | *--arp-type ARP* | ...genera i envia (per defecte, cinc) paquets ARP de petició de tipus broadcast preguntant la MAC de la IP indicada |
| | *--arp-type ARP-reply* | ...genera i envia (per defecte, cinc) paquets ARP de resposta a la IP indicada informant de la MAC i IP pròpia |

NOTA: Altres paràmetres que es poden afegir a *--arp* i *--arp-type* són *--arp-sender-mac=<mac>* (que estableix la MAC d'origen del paquet -en lloc de la real-) i *--arp-sender-ip=<addr>* (que estableix la IP d'origen -en lloc de la real-). Aquests dos paràmetres són interessants si es vol fer un atac de tipus "ARP-Spoofing", per exemple

*--icmp* Indica que es vol enviar paquet/s ICMP, on ...

*--icmp-type nº* ...especifica el tipus de paquet ICMP a enviar

Si el "valor" és 8, s'enviarà un paquet de tipus "Echo request"

Si el "valor" és 0, s'enviarà un paquet de tipus "Echo reply"

*--icmp-code nº* ...especifica el codi del paquet ICMP a enviar

Pels missatges de tipus "Echo request" o "Echo reply" val 0

*-p nº,nº-nº* Indica els ports de destí on s'enviarà el paquet generat (sols si és UDP/TCP)

*--udp* Indica que es vol enviar paquet/s UDP

*--tcp* Indica que es vol enviar paquet/s TCP

*--flags {syn,ack,rst,fin,urg,psh}* Indica quin/s flag/s tindran activat/s aquests paquets

*--seq nº* Estableix el nº de seqüència del paquet

*--ack nº* Estableix el nº d'acusament del paquet

*--win nº* Estableix el tamany (en bytes) de la finestra TCP

*--data valorsHexadecimals* Estableix el valor del "payload" del paquet (en hexadecimal)

*--data-string "cadena"* Estableix el valor del "payload" del paquet (com a cadena)

*--data-length nº* Indica el tamany (en bytes) del "payload", que serà aleatori

NOTA: Altres paràmetres no tan habituals de *nping* però també interessants són:

*--ttl nº* Especifica el TTL dels paquets IP (ja siguin ICMP, TCP o UDP)

*-g nº* Especifica el port d'origen del paquet (això només si és UDP o TCP)

*--dest-mac xx:xx:xx:xx:xx:xx* Indica la direcció MAC de destí (deshabilita la resolució ARP, doncs)

*--source-mac xx:xx:xx:xx:xx:xx* Indica (falseja) la direcció MAC d'origen

*--badsum-ip* o *--badsum* Crea un paquet IP o ICMP/TCP/UDP malformat, respectivament

*--tcp-connect* Genera quatre paquets de conexió 3-way handshake (per defecte al port de destí 80)