

1.-

Per veure les connexions TCP actives al Windows, podem utilitzar l'ordre `netstat -an | findstr /s tcp`. Aquesta ordre proporciona una llista de totes les connexions actives usant el protocol TCP, detallant l'adreça local (IP i el port d'origen), l'adreça remota (IP i el port de destinació) i l'estat de la connexió. Els ports TCP que estiguin esperant connexions apareixeran en estat LISTENING, els que tinguin una connexió establerta apareixeran com a ESTABLISHED, i aquells que esperen que es processin els paquets finals després de tancar-se tindran l'estat TIME\_WAIT.

```

C:\Users\c1775216>netstat -an | findstr /i tcp
TCP    0.0.0.0:135          0.0.0.0:0          LISTENING
TCP    0.0.0.0:445          0.0.0.0:0          LISTENING
TCP    0.0.0.0:3389         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5040         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5357         0.0.0.0:0          LISTENING
TCP    0.0.0.0:8000         0.0.0.0:0          LISTENING
TCP    0.0.0.0:8032         0.0.0.0:0          LISTENING
TCP    0.0.0.0:11100        0.0.0.0:0          LISTENING
TCP    0.0.0.0:30950        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49664        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49665        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49666        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49667        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49668        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49669        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49670        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49682        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49684        0.0.0.0:0          LISTENING
TCP    127.0.0.1:5354       0.0.0.0:0          LISTENING
TCP    127.0.0.1:10398      0.0.0.0:0          LISTENING
TCP    127.0.0.1:10398      127.0.0.1:49857    ESTABLISHED
TCP    127.0.0.1:11200      0.0.0.0:0          LISTENING
TCP    127.0.0.1:11300      0.0.0.0:0          LISTENING
TCP    127.0.0.1:11300      127.0.0.1:49764    ESTABLISHED
TCP    127.0.0.1:49764      127.0.0.1:11300    ESTABLISHED
TCP    127.0.0.1:49841      0.0.0.0:0          LISTENING
TCP    127.0.0.1:49841      127.0.0.1:63978    ESTABLISHED
TCP    127.0.0.1:49842      0.0.0.0:0          LISTENING
TCP    127.0.0.1:49842      127.0.0.1:49844    ESTABLISHED
TCP    127.0.0.1:49844      127.0.0.1:49842    ESTABLISHED
TCP    127.0.0.1:49857      127.0.0.1:10398    ESTABLISHED
TCP    127.0.0.1:50038      127.0.0.1:50039    ESTABLISHED
TCP    127.0.0.1:50039      127.0.0.1:50038    ESTABLISHED
TCP    127.0.0.1:50919      0.0.0.0:0          LISTENING
TCP    127.0.0.1:54672      127.0.0.1:49841    TIME_WAIT
TCP    127.0.0.1:54675      127.0.0.1:54676    ESTABLISHED
TCP    127.0.0.1:54676      127.0.0.1:54675    ESTABLISHED
TCP    127.0.0.1:54677      127.0.0.1:54678    ESTABLISHED
TCP    127.0.0.1:54678      127.0.0.1:54677    ESTABLISHED
TCP    127.0.0.1:58599      127.0.0.1:49841    TIME_WAIT
TCP    127.0.0.1:61829      127.0.0.1:49841    TIME_WAIT
TCP    127.0.0.1:62430      127.0.0.1:49841    TIME_WAIT
TCP    127.0.0.1:63978      127.0.0.1:49841    ESTABLISHED
TCP    192.168.56.1:139     0.0.0.0:0          LISTENING
TCP    192.168.88.251:139   0.0.0.0:0          LISTENING
TCP    192.168.88.251:62076 147.83.194.6:5444   ESTABLISHED
TCP    192.168.88.251:62429 192.168.88.1:53     TIME_WAIT
TCP    192.168.88.251:62431 2.20.187.99:443     ESTABLISHED
TCP    192.168.88.251:63977 192.168.88.1:53     SYN_SENT
TCP    [::]:135             [::]:0             LISTENING
TCP    [::]:445             [::]:0             LISTENING
TCP    [::]:3389            [::]:0             LISTENING
TCP    [::]:5357            [::]:0             LISTENING
TCP    [::]:8032            [::]:0             LISTENING
TCP    [::]:11100           [::]:0             LISTENING
TCP    [::]:49664           [::]:0             LISTENING
TCP    [::]:49665           [::]:0             LISTENING
TCP    [::]:49666           [::]:0             LISTENING
TCP    [::]:49667           [::]:0             LISTENING
TCP    [::]:49668           [::]:0             LISTENING
TCP    [::]:49669           [::]:0             LISTENING
TCP    [::]:49670           [::]:0             LISTENING
TCP    [::]:49682           [::]:0             LISTENING

```

D'altra banda, per veure les connexions UDP actives, podem fer servir netstat -an | findstr /s udp, la qual cosa mostrarà les connexions UDP actives i els ports oberts a UDP, encara que, com que és un protocol sense connexió, no veurem estats com en TCP.

```
C:\Users\c1775216>netstat -an | findstr /i udp
UDP    0.0.0.0:123          *:*
UDP    0.0.0.0:500          *:*
UDP    0.0.0.0:1434         *:*
UDP    0.0.0.0:3389         *:*
UDP    0.0.0.0:3702         *:*
UDP    0.0.0.0:3702         *:*
UDP    0.0.0.0:4500         *:*
UDP    0.0.0.0:5050         *:*
UDP    0.0.0.0:5353         *:*
UDP    0.0.0.0:5355         *:*
UDP    0.0.0.0:52455        *:*
UDP    0.0.0.0:56969        *:*
UDP    0.0.0.0:60218        *:*
UDP    0.0.0.0:60610        *:*
UDP    127.0.0.1:1900        *:*
UDP    127.0.0.1:51128       *:*
UDP    127.0.0.1:51131       *:*
UDP    127.0.0.1:56460       *:*
UDP    192.168.56.1:137      *:*
UDP    192.168.56.1:138      *:*
UDP    192.168.56.1:1900     *:*
UDP    192.168.56.1:5353     *:*
UDP    192.168.56.1:56458    *:*
UDP    192.168.88.251:137    *:*
UDP    192.168.88.251:138    *:*
UDP    192.168.88.251:1900   *:*
UDP    192.168.88.251:5353   *:*
UDP    192.168.88.251:56459 *:*
UDP    [::]:123              *:*
UDP    [::]:500              *:*
UDP    [::]:1434             *:*
UDP    [::]:3389             *:*
UDP    [::]:3702             *:*
UDP    [::]:3702             *:*
UDP    [::]:4500             *:*
UDP    [::]:5353             *:*
UDP    [::]:5355             *:*
UDP    [::]:52456            *:*
UDP    [::]:56970            *:*
UDP    [::]:60218            *:*
UDP    [::]:60610            *:*
UDP    [::1]:1900            *:*
UDP    [::1]:5353            *:*
UDP    [::1]:56457           *:*
UDP    [fe80::43be:468c:94b3:970a%13]:1900 *:*
UDP    [fe80::43be:468c:94b3:970a%13]:56456 *:*
UDP    [fe80::46c8:4f72:25c3:e672%14]:1900 *:*
UDP    [fe80::46c8:4f72:25c3:e672%14]:56455 *:*
```

Amb l'ordre `netstat -an | findstr /i listening`, podem obtenir un llistat dels ports que estan en estat d'escolta (LISTENING). Aquest estat indica que el port està obert i esperant connexions entrants, per la qual cosa el sistema operatiu està preparat per acceptar sol·licituds externes a aquests ports.

```
C:\Users\c1775216>netstat -an | findstr /i listening
TCP    0.0.0.0:135          0.0.0.0:0          LISTENING
TCP    0.0.0.0:445          0.0.0.0:0          LISTENING
TCP    0.0.0.0:3389         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5040         0.0.0.0:0          LISTENING
TCP    0.0.0.0:5357         0.0.0.0:0          LISTENING
TCP    0.0.0.0:8000         0.0.0.0:0          LISTENING
TCP    0.0.0.0:8032         0.0.0.0:0          LISTENING
TCP    0.0.0.0:11100        0.0.0.0:0          LISTENING
TCP    0.0.0.0:30950        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49664        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49665        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49666        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49667        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49668        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49669        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49670        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49682        0.0.0.0:0          LISTENING
TCP    0.0.0.0:49684        0.0.0.0:0          LISTENING
TCP    127.0.0.1:5354       0.0.0.0:0          LISTENING
TCP    127.0.0.1:10398      0.0.0.0:0          LISTENING
TCP    127.0.0.1:11200      0.0.0.0:0          LISTENING
TCP    127.0.0.1:11300      0.0.0.0:0          LISTENING
TCP    127.0.0.1:49841      0.0.0.0:0          LISTENING
TCP    127.0.0.1:49842      0.0.0.0:0          LISTENING
TCP    127.0.0.1:50919      0.0.0.0:0          LISTENING
TCP    192.168.56.1:139     0.0.0.0:0          LISTENING
TCP    192.168.88.251:139   0.0.0.0:0          LISTENING
TCP    [::]:135            [::]:0             LISTENING
TCP    [::]:445            [::]:0             LISTENING
TCP    [::]:3389           [::]:0             LISTENING
TCP    [::]:5357           [::]:0             LISTENING
TCP    [::]:8032           [::]:0             LISTENING
TCP    [::]:11100          [::]:0             LISTENING
TCP    [::]:49664          [::]:0             LISTENING
TCP    [::]:49665          [::]:0             LISTENING
TCP    [::]:49666          [::]:0             LISTENING
TCP    [::]:49667          [::]:0             LISTENING
TCP    [::]:49668          [::]:0             LISTENING
TCP    [::]:49669          [::]:0             LISTENING
TCP    [::]:49670          [::]:0             LISTENING
TCP    [::]:49682          [::]:0             LISTENING
TCP    [::]:49684          [::]:0             LISTENING
TCP    [::1]:49672         [::]:0             LISTENING
```

2.-

Quan fem un escaneig de ports utilitzant Telnet, el protocol de transport que es fa servir és TCP. Telnet estableix connexions de forma fiable a través de TCP, cosa que garanteix que les dades s'enviïn i rebin correctament. Durant l'escaneig, Telnet intenta connectar-se a un port específic en un host remot, en el nostre cas la màquina virtual; si la connexió s'estableix, indica que el port està obert mentre que un missatge d'error suggereix que el port està tancat. Aquesta confiança i control en la transmissió fan de TCP el protocol ideal per a aquest tipus d'interaccions.

A la següent imatge podem veure com telnet estableix connexió mitjançant TCP.

The image shows a Wireshark packet capture window titled "Capturing from Ethernet 2 [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]". The filter is set to "ip.addr==192.168.88.250". The packet list shows a series of packets from 192.168.88.250 to 192.168.88.251. The first packet (No. 193) is a TCP SYN packet (Seq=0, Ack=1, Win=29200, Len=0, MSS=1460). The second packet (No. 195) is a TCP ACK packet (Seq=1, Ack=22, Win=29216, Len=0). The third packet (No. 233) is a TELNET Data packet. The fourth packet (No. 234) is a TELNET Data packet. The fifth packet (No. 235) is a TELNET Data packet. The sixth packet (No. 236) is a TCP ACK packet (Seq=43, Ack=68, Win=29216, Len=0). The seventh packet (No. 237) is a TELNET Data packet. The eighth packet (No. 238) is a TCP ACK packet (Seq=52, Ack=77, Win=29216, Len=0). The ninth packet (No. 239) is a TELNET Data packet. The tenth packet (No. 240) is a TELNET Data packet. The eleventh packet (No. 349) is a TELNET Data packet. The twelfth packet (No. 350) is a TCP FIN packet (Seq=137, Ack=77, Win=29216, Len=0). The thirteenth packet (No. 351) is a TCP ACK packet (Seq=138, Ack=78, Win=29216, Len=0). The packet details pane shows the selected packet (No. 193) with the following details: Frame 193: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0; Ethernet II, Src: cadmusco\_ce:b9:5b (08:00:27:ce:b9:5b), Dst: 6c:4b:90:c1:68:68 (6c:4b:90:c1:68:68); Internet Protocol Version 4, Src: 192.168.88.250 (192.168.88.250), Dst: 192.168.88.251 (192.168.88.251); Transmission Control Protocol, Src Port: 23 (23), Dst Port: 62211 (62211), Seq: 0, Ack: 1, Len: 0. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
193	69.53344800	192.168.88.250	192.168.88.251	TCP	66	23-62211 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 S...
195	69.53654100	192.168.88.250	192.168.88.251	TCP	60	23-62211 [ACK] Seq=1 Ack=22 win=29216 Len=0
233	79.54926600	192.168.88.250	192.168.88.251	TELNET	66	Telnet Data ...
234	79.55118300	192.168.88.250	192.168.88.251	TELNET	66	Telnet Data ...
235	79.55172800	192.168.88.250	192.168.88.251	TELNET	72	Telnet Data ...
236	79.55250200	192.168.88.250	192.168.88.251	TCP	60	23-62211 [ACK] Seq=43 Ack=68 win=29216 Len=0
237	79.55300900	192.168.88.250	192.168.88.251	TELNET	63	Telnet Data ...
238	79.55376600	192.168.88.250	192.168.88.251	TCP	60	23-62211 [ACK] Seq=52 Ack=77 win=29216 Len=0
239	79.56245400	192.168.88.250	192.168.88.251	TELNET	74	Telnet Data ...
240	79.60329600	192.168.88.250	192.168.88.251	TELNET	82	Telnet Data ...
349	139.56501400	192.168.88.250	192.168.88.251	TELNET	91	Telnet Data ...
350	139.56512900	192.168.88.250	192.168.88.251	TCP	60	23-62211 [FIN, ACK] Seq=137 Ack=77 win=29216 Len=0
351	139.56590700	192.168.88.250	192.168.88.251	TCP	60	23-62211 [ACK] Seq=138 Ack=78 win=29216 Len=0

Frame 193: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0  
Ethernet II, Src: cadmusco\_ce:b9:5b (08:00:27:ce:b9:5b), Dst: 6c:4b:90:c1:68:68 (6c:4b:90:c1:68:68)  
Internet Protocol Version 4, Src: 192.168.88.250 (192.168.88.250), Dst: 192.168.88.251 (192.168.88.251)  
Transmission Control Protocol, Src Port: 23 (23), Dst Port: 62211 (62211), Seq: 0, Ack: 1, Len: 0

0000 6c 4b 90 c1 68 68 08 00 27 ce b9 5b 08 00 45 00 1k..hh.. '...E.  
0010 00 34 00 00 40 00 06 07 7e c0 a8 58 fa c0 a8 .4...@. ...X..  
0020 58 fb 00 17 f3 03 a9 cf 07 6a 97 71 bd 8c 80 12 x.....j.q....  
0030 72 10 d0 59 00 00 02 04 05 b4 01 01 04 02 01 03 r..Y.....  
0040 03 05 ..

Ethernet 2: <live capture in progress> File: C:... Packets: 353 - Displayed: 13 (3.7%) Profile: Default

3.-

- Ports UDP: Telnet funciona sobre TCP, per la qual cosa no pot escanejar ports UDP, ja que aquests protocols no estableixen connexions orientades a la connexió.
- Ports que no accepten connexions: Alguns ports poden estar tancats i no acceptar connexions.
- Ports filtrats: Si hi ha un tallafocs o un sistema de prevenció d'intrusions a la xarxa que bloqueja el trànsit cap a certs ports.
- Serveis que requereixen autenticació o protocols específics: Alguns serveis, com els de correu electrònic (SMTP al port 25) o servidors web que requereixen HTTPS (port 443), poden no respondre correctament si s'intenta accedir-hi de manera genèrica amb Telnet, ja que poden esperar ordres específiques o requerir xifrat.

- Ports de serveis no interactius: Alguns ports poden estar associats amb serveis que no tenen una interfície interactiva (com certs serveis de base de dades).

4.-

Quan fem un escaneig de ports i el port està obert, com el port 80 (que s'utilitza comunament per al trànsit HTTP), s'estableix una connexió TCP entre l'escàner i el servei al port. Durant aquest procés, l'escàner intenta enviar un paquet de connexió al port específic i, si està obert, el sistema remot accepta la connexió. Això és un indicador clau que el servei associat al port està disponible i operatiu.

Un cop establerta la connexió, el servei que escolta al port, en aquest cas, un servidor web, pot respondre a la sol·licitud realitzada per l'escàner. El servidor respondrà amb informació rellevant, que pot incloure el codi d'estat HTTP, encapçalats i, potencialment, contingut HTML. Aquesta interacció permet als administradors verificar que el servei funciona correctament.

El client telnet inicia la connexió enviant un paquet amb el flag SYN activat, indicant el seu desig de connectar-se i enviant un número de seqüència inicial. En resposta, el servidor envia un paquet amb tots dos flags SYN i ACK, reconeixent la sol·licitud del client i proporcionant el seu propi número de seqüència. Finalment, el client respon amb un paquet ACK per confirmar la recepció del missatge del servidor.

Capturing from Ethernet 2 [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.88.250` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
52	25.67151900	192.168.88.250	192.168.88.251	TCP	66	80→62439 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1460 S
53	25.67534700	192.168.88.250	192.168.88.251	TCP	60	80→62439 [ACK] Seq=1 Ack=22 win=29216 Len=0

Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: CadmusCo\_ce:b9:5b (08:00:27:ce:b9:5b), Dst: 6c:4b:90:c1:68:68 (6c:4b:90:c1:68:68)

Internet Protocol Version 4, Src: 192.168.88.250 (192.168.88.250), Dst: 192.168.88.251 (192.168.88.251)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62439 (62439), Seq: 0, Ack: 1, Len: 0

```

0000  6c 4b 90 c1 68 68 08 00 27 ce b9 5b 08 00 45 00  1k..hh.. '...[.E.
0010  00 34 00 00 40 00 40 06 07 7e c0 a8 58 fa c0 a8  .4..@.@. ~..X...
0020  58 fb 00 50 f3 e7 1b c8 03 bc b0 c4 c2 73 80 12  X..P.... ..S..
0030  72 10 42 b8 00 00 02 04 05 b4 01 01 04 02 01 03  r.B..... ..
0040  03 05  ..

```

Ethernet 2: <live capture in progress> File: C:\... Packets: 72 - Displayed: 2 (2.8%) Profile: Default

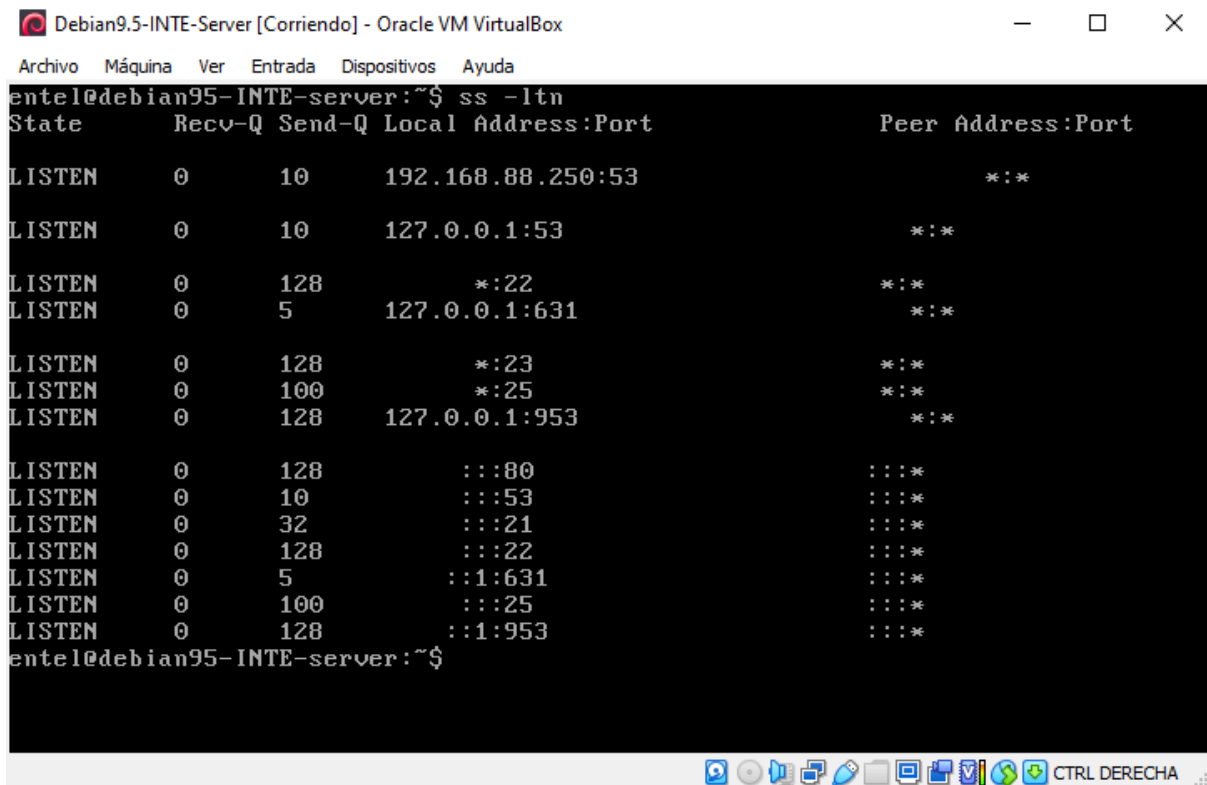
5.-

#### Ports TCP

- Port 21 (FTP): Utilitzat per a la transferència de fitxers, permetent la pujada i descàrrega de fitxers entre un client i un servidor.
- Port 22 (SSH): Protocol de xarxa per a l'accés segur a sistemes remots, permet l'administració i el control segur.
- Port 25 (SMTP): Utilitzat per enviar correus electrònics entre servidors.
- Port 80 (HTTP): Usat per servidors web per servir contingut a navegadors a través del protocol HTTP.
- Port 953 (BIND): Usat per a l'administració i control del servidor DNS.
- Port 631 (IPP): Protocol utilitzat per a la impressió en xarxa.
- Ports 41168 i 56930: Aquests són ports dinàmics, que generalment són utilitzats per aplicacions per establir connexions temporals, i el seu ús específic pot variar segons l'aplicació que els utilitzeu.

#### Ports UDP

- Port 53 (DNS): Usat pel sistema de noms de domini per resoldre noms de domini en adreces IP.
- Port 68 (DHCP Client): Utilitzat pels clients DHCP per rebre adreces IP i configuració de xarxa d'un servidor DHCP.
- Port 5353 (mDNS): Usat per a la resolució de noms en una xarxa local sense necessitat d'un servidor DNS.
- Ports 41168 i 56930: Aquests són ports dinàmics, que generalment són utilitzats per aplicacions per establir connexions temporals, i el seu ús específic pot variar segons l'aplicació que els utilitzeu.



```
Debian9.5-INTE-Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
entel@debian95-INTE-server:~$ ss -ltn
State      Recv-Q  Send-Q  Local Address:Port      Peer Address:Port
LISTEN     0        10      192.168.88.250:53        *:*
LISTEN     0        10      127.0.0.1:53            *:*
LISTEN     0       128          *:22                    *:*
LISTEN     0         5      127.0.0.1:631           *:*
LISTEN     0       128          *:23                    *:*
LISTEN     0      100          *:25                    *:*
LISTEN     0       128     127.0.0.1:953           *:*
LISTEN     0       128          :::80                   :::*
LISTEN     0         10          :::53                   :::*
LISTEN     0        32          :::21                   :::*
LISTEN     0       128          :::22                   :::*
LISTEN     0         5          :::1:631                 :::*
LISTEN     0      100          :::25                   :::*
LISTEN     0       128          :::1:953                 :::*
entel@debian95-INTE-server:~$
```



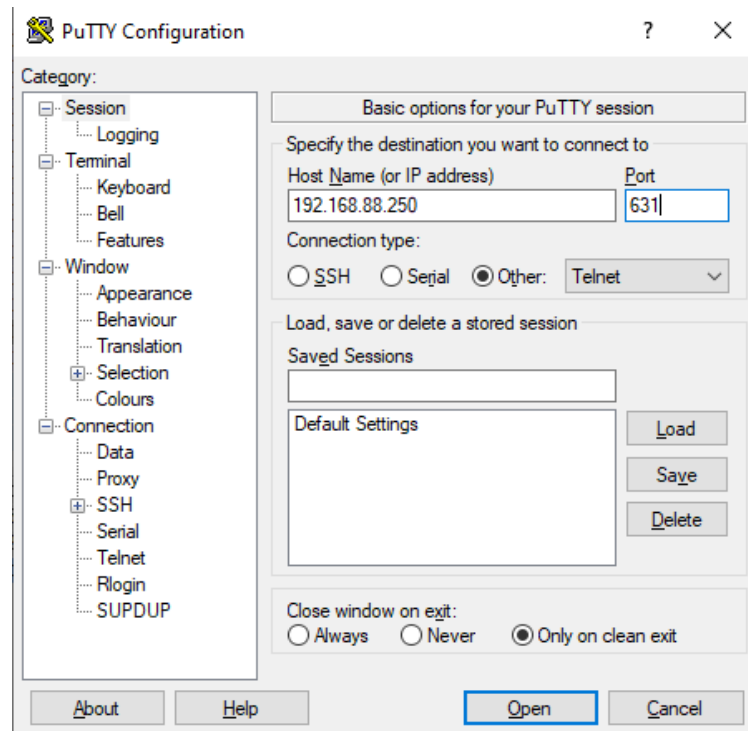
```

entel@debian95-INTE-server:~$ ss -ltn
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
UNCONN     0      0      *:631                  *::*
UNCONN     0      0      *:41168                *::*
UNCONN     0      0      *:5353                 *::*
UNCONN     0      0      192.168.88.250:53      *::*
UNCONN     0      0      127.0.0.1:53          *::*
UNCONN     0      0      *:68                   *::*
UNCONN     0      0      :::56930               :::*
UNCONN     0      0      :::5353                :::*
UNCONN     0      0      :::53                  :::*
entel@debian95-INTE-server:~$ _

```

6.-

Si realitzem un escaneig de ports a un port que no està obert, des d'un sistema Linux rebrà un error de connexió, ja que no podrà establir la connexió amb el port tancat de la màquina virtual (VM).



Utilitzant Wireshark, podem observar l'intercanvi de paquets que es produeix durant aquest procés. La seqüència seria la següent:



1. Host Linux → SYN → Host VM: El host Linux inicia la connexió enviant un paquet TCP amb la bandera SYN activada al host VM.
2. Host Linux ← RST-ACK ← Host VM: Com a resposta al paquet SYN, la VM, en no reconèixer la petició del Linux, rebutja l'establiment de la connexió enviant un paquet
3. RST-ACK.

The screenshot shows two windows. On the left is Wireshark, capturing traffic on interface 0. The filter is set to 'ip.addr==192.168.88.250'. The packet list shows four packets: a SYN packet (Seq=1) and three RST-ACK packets (Seq=1, Ack=1). The packet details for the first packet (Frame 7) show it's a TCP segment with Seq=1, Ack=1, Win=0, and Len=0. On the right is a PuTTY window titled '192.168.88.250 - PuTTY'. It displays a 'PuTTY Fatal Error' dialog box with the message 'Network error: Connection refused' and an 'Aceptar' button.

El camp RST significa "reset", i indica que la connexió s'ha restablert, refusant la petició de connexió. Això implica que el port no està disponible i que la màquina virtual no acceptarà cap connexió a través d'aquest port.

7.-

Es poden trobar dins del paquet SYN, en el context del protocol TCP, quan el host A envia un paquet SYN al host B, aquest paquet és essencial per establir les característiques de la connexió. El paquet SYN conté informació que el host B pot acceptar o rebutjar, permetent així la negociació dels paràmetres de la connexió.

```
[Destination GeoIP: UNKNOWN]
Transmission Control Protocol, Src Port: 62923 (62923), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 62923 (62923)
  Destination Port: 80 (80)
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 32 bytes
  ... 0000 0000 0010 = Flags: 0x002 (SYN)
  window size value: 64240
  [Calculated window size: 64240]
  Checksum: 0x66c4 [validation disabled]
  Urgent pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    Maximum segment size: 1460 bytes
    No-Operation (NOP)
    window scale: 8 (multiply by 256)
    No-Operation (NOP)
    No-Operation (NOP)
    TCP SACK Permitted Option: True
```

Podem identificar que el paquet és un SYN perquè té activada la flag de SYN (0x02). En analitzar les dades d'aquest paquet, és possible observar les opcions TCP que ofereix el host A. Algunes d'aquestes opcions poden ser:

- Màxima mida del segment (MSS): Per exemple, 1460 bytes, per evitar la fragmentació durant la transmissió de dades.
- Permissió del SACK: Indica si es permet el Selective Acknowledgment, una funcionalitat que millora l'eficiència en cas de pèrdua de paquets.
- Timestamps: Utilitzades per mesurar el temps de viatge rodó (RTT) i millorar el rendiment de la connexió.
- No-operation: Aquesta opció serveix com a relleno per assegurar que les altres opcions estiguin correctament alineades.
- Número màxim de la finestra: En aquest cas, es pot especificar un valor com 7 x 128, que equival a 896 bytes, definint així la capacitat màxima que el host A està disposat a acceptar per la recepció de dades.

Aquestes opcions poden variar depenent de les configuracions dels host i dels paràmetres negociats, per la qual cosa no tots els paquets SYN presentaran les mateixes opcions.

8.-

El Retransmission TimeOut (RTO) inicial en TCP es determina durant la fase de three-way handshake que s'utilitza per establir la connexió. Aquest valor es calcula basant-se en les mesures del Round-Trip Time (RTT), sempre que hi hagi dades suficients per fer aquesta avaluació. Si no es disposa de les dades necessàries per calcular el RTT, TCP recorrerà a un valor predeterminat, que pot variar depenent del sistema operatiu. En general, aquest valor predeterminat se sol situar entre 0 i 3 segons.

9.-

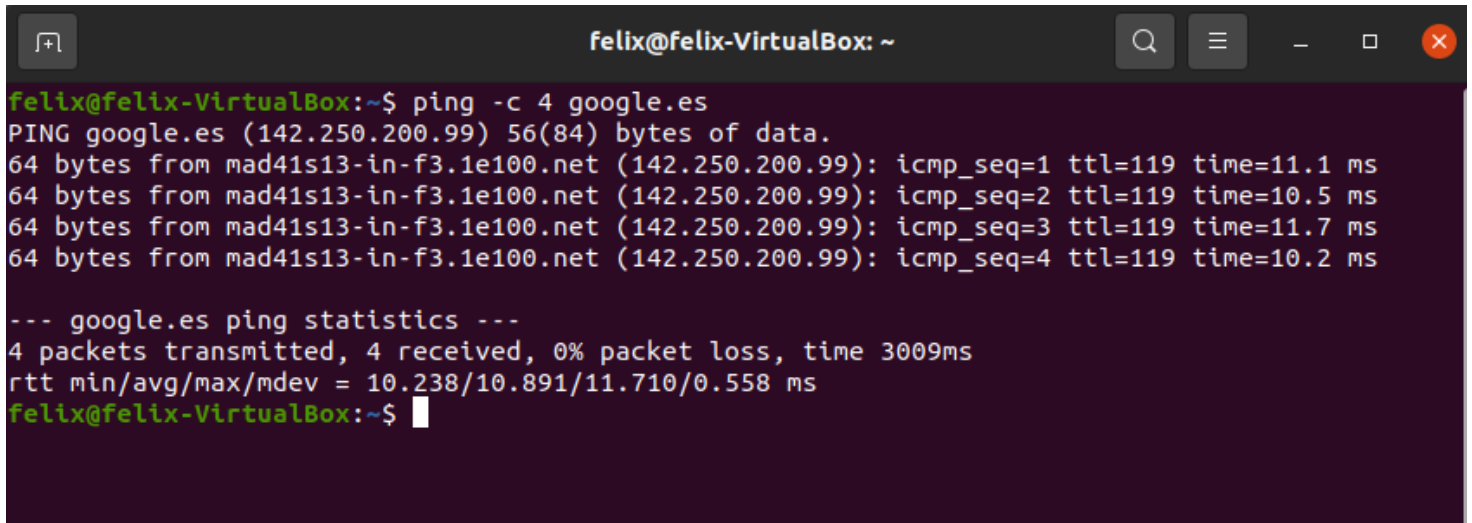
Per determinar el nombre màxim de retransmissions d'un sistema operatiu, podem utilitzar les següents instruccions:

En un sistema operatiu Unix/Linux, podem executar la comanda `sysctl` amb el paràmetre `net.ipv4.tcp_retries2`. Aquest paràmetre especifica el nombre màxim de retransmissions TCP que es realitzaran durant un intent d'establir una connexió abans de considerar que la contrapart no està disponible.

```
felix@felix-VirtualBox:~$ sysctl net.ipv4.tcp_retries2
net.ipv4.tcp_retries2 = 15
felix@felix-VirtualBox:~$
```

Per exemple, si el valor és 15, significa que el nucli del sistema està configurat per intentar retransmetre paquets TCP fins a 15 vegades abans de concloure que la connexió ha fallat. Aquesta configuració és fonamental per garantir la fiabilitat i el control de congestió en les connexions TCP. Un valor elevat per a `tcp_retries2` pot permetre més temps per

recuperar-se en condicions de xarxa inestables, però també pot implicar un temps d'espera més llarg abans que l'aplicació sigui informada de la fallada de la connexió.

A screenshot of a terminal window titled 'felix@felix-VirtualBox: ~'. The terminal shows the execution of a ping command: 'ping -c 4 google.es'. The output displays four successful ping responses from 'mad41s13-in-f3.1e100.net' (142.250.200.99) with varying round-trip times (11.1 ms, 10.5 ms, 11.7 ms, 10.2 ms). Below the individual responses, it shows '--- google.es ping statistics ---', indicating 4 packets transmitted, 4 received, 0% packet loss, and a total time of 3009ms. The final line shows the round-trip time statistics: 'rtt min/avg/max/mdev = 10.238/10.891/11.710/0.558 ms'. The prompt 'felix@felix-VirtualBox:~\$' is visible at the bottom.

```
felix@felix-VirtualBox:~$ ping -c 4 google.es
PING google.es (142.250.200.99) 56(84) bytes of data.
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=1 ttl=119 time=11.1 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=2 ttl=119 time=10.5 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=3 ttl=119 time=11.7 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=4 ttl=119 time=10.2 ms

--- google.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 10.238/10.891/11.710/0.558 ms
felix@felix-VirtualBox:~$
```

A més, la sortida d'una comanda ping executada en una terminal pot mostrar el temps que cada paquet ha trigat a fer un viatge d'anada i tornada a un host destinatari, conegut com a Round-Trip Time (RTT). En un exemple, els resultats poden mostrar valors com 11.1ms, 10.5ms... I també al final de la transmissió podem veure el rtt mínim, promig, màxim...

10.-

Els valors per defecte dels paràmetres de TCP depenen principalment del sistema operatiu, ja que cadascú té la seva pròpia implementació de TCP i estableix configuracions predeterminades, com la mida de la finestra, el temps d'espera de connexió i la mida màxima de transmissió (MTU). Aquests valors poden variar entre diferents sistemes operatius, i poden ser ajustats pels administradors de sistemes segons les necessitats específiques de l'entorn.

Tot i que les aplicacions que utilitzen TCP poden optimitzar-ne el comportament dins d'aquests paràmetres, generalment segueixen els valors predeterminats establerts pel sistema operatiu.