**GESTION DES RISQUES INFORMATIQUES**

**DESS en Technologie de l'Information**

# EXERCICES D’APPLICATION

Etudiant : Stanley LAFLEUR

netstat est un outil puissant pour surveiller les connexions réseau, les ports ouverts et les statistiques réseau. Voici des exercices pratiques avec corrections pour mieux comprendre son utilisation.

Taper la commande **netstat help,** pour découvrir le manuel sur netstat. Servez-vous de ce manuel pour répondre aux questions suivantes.

1. Lister toutes les connexions réseau actives

C:\Windows\system32>netstat -a

Active Connections

Proto Local Address Foreign Address State

TCP 0.0.0.0:135 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:445 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:5040 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:5357 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49664 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49665 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49666 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49667 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49668 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49670 DESKTOP-P5EIGGR:0 LISTENING

TCP 127.0.0.1:8884 DESKTOP-P5EIGGR:0 LISTENING

TCP 172.20.10.4:139 DESKTOP-P5EIGGR:0 LISTENING

TCP 172.20.10.4:50137 13.86.221.35:https TIME\_WAIT

TCP 172.20.10.4:50143 172.172.255.217:https ESTABLISHED

TCP 172.20.10.4:50146 20.190.190.196:https TIME\_WAIT

TCP 172.20.10.4:50148 172.172.255.217:https ESTABLISHED

TCP 172.20.10.4:50152 20.54.232.160:https TIME\_WAIT

TCP 172.20.10.4:50153 20.190.190.196:https TIME\_WAIT

TCP 172.20.10.4:50156 20.169.174.231:https ESTABLISHED

TCP 172.20.10.4:50157 13.91.58.244:https TIME\_WAIT

TCP 172.20.10.4:50165 13.91.58.244:https ESTABLISHED

TCP 172.20.10.4:50167 a23-207-52-43:https TIME\_WAIT

TCP 172.20.10.4:50171 199.232.210.172:http TIME\_WAIT

TCP 172.20.10.4:50175 52.123.129.14:https TIME\_WAIT

TCP 172.20.10.4:50179 52.112.100.63:https TIME\_WAIT

TCP 172.20.10.4:50181 150.171.28.11:https ESTABLISHED

TCP 172.20.10.4:50184 13.107.3.128:https TIME\_WAIT

TCP 172.20.10.4:50185 4.172.12.147:https ESTABLISHED

TCP 172.20.10.4:50186 52.112.122.33:https ESTABLISHED

TCP 172.20.10.4:50187 52.112.72.35:https ESTABLISHED

TCP 172.20.10.4:50191 20.42.65.84:https TIME\_WAIT

TCP 172.20.10.4:50192 52.112.87.198:https TIME\_WAIT

TCP 172.20.10.4:50193 52.112.87.198:https TIME\_WAIT

TCP 172.20.10.4:50194 104.18.32.47:https TIME\_WAIT

TCP 172.20.10.4:50195 104.18.32.47:https ESTABLISHED

TCP 172.20.10.4:50198 52.112.100.56:https ESTABLISHED

TCP 172.20.10.4:50199 52.112.238.173:https TIME\_WAIT

TCP 172.20.10.4:50203 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50204 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50205 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50206 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50207 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50208 a104-70-121-185:https CLOSE\_WAIT

TCP 172.20.10.4:50211 a184-31-62-37:https ESTABLISHED

TCP 172.20.10.4:50213 20.190.152.20:https ESTABLISHED

TCP 172.20.10.4:50215 20.190.152.20:https ESTABLISHED

TCP 172.20.10.4:50224 20.50.80.210:https TIME\_WAIT

TCP 172.20.10.4:50226 20.42.65.88:https ESTABLISHED

TCP 172.20.10.4:50227 whatsapp-chatd-edge-shv-01-mia3:5222 TIME\_WAIT

TCP 172.20.10.4:50228 52.182.143.215:https ESTABLISHED

TCP 172.20.10.4:50230 200.113.232.99:https ESTABLISHED

TCP 172.20.10.4:50231 200.113.232.225:https ESTABLISHED

TCP 172.20.10.4:50233 200.113.232.225:https ESTABLISHED

TCP 172.20.10.4:50235 150.171.28.11:https ESTABLISHED

TCP 172.20.10.4:50236 52.96.111.98:https ESTABLISHED

TCP 172.20.10.4:50237 52.96.111.98:https ESTABLISHED

TCP 172.20.10.4:50238 52.111.229.57:https ESTABLISHED

TCP 172.20.10.4:50239 bingforbusiness:https ESTABLISHED

TCP 172.20.10.4:50240 20.69.137.228:https ESTABLISHED

TCP 172.20.10.4:50244 172.64.155.209:https ESTABLISHED

TCP 172.20.10.4:50245 whatsapp-chatd-edge-shv-01-mia3:5222 TIME\_WAIT

TCP 172.20.10.4:50246 whatsapp-chatd-edge-shv-01-mia3:5222 TIME\_WAIT

TCP 172.20.10.4:50247 ec2-3-233-158-24:https ESTABLISHED

TCP 172.20.10.4:50248 8.243.166.91:http ESTABLISHED

TCP 172.20.10.4:50249 whatsapp-chatd-edge-shv-01-mia3:5222 TIME\_WAIT

TCP 172.20.10.4:50250 whatsapp-chatd-edge-shv-01-mia3:5222 ESTABLISHED

TCP 172.20.10.4:50251 whatsapp-cdn-shv-01-mia3:https ESTABLISHED

TCP [::]:135 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:445 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:5357 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49664 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49665 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49666 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49667 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49668 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49670 DESKTOP-P5EIGGR:0 LISTENING

TCP [::1]:42050 DESKTOP-P5EIGGR:0 LISTENING

TCP [::1]:49669 DESKTOP-P5EIGGR:0 LISTENING

UDP 0.0.0.0:123 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:3702 \*:\*

UDP 0.0.0.0:5050 \*:\*

UDP 0.0.0.0:5353 \*:\*

UDP 0.0.0.0:5353 \*:\*

UDP 0.0.0.0:5353 \*:\*

UDP 0.0.0.0:5355 \*:\*

UDP 0.0.0.0:50072 \*:\*

UDP 0.0.0.0:50085 \*:\*

UDP 0.0.0.0:51301 \*:\*

UDP 0.0.0.0:57202 \*:\*

UDP 0.0.0.0:57843 \*:\*

UDP 0.0.0.0:60634 \*:\*

UDP 127.0.0.1:1900 \*:\*

UDP 127.0.0.1:49664 \*:\*

UDP 127.0.0.1:50479 \*:\*

UDP 127.0.0.1:52033 \*:\*

UDP 172.20.10.4:137 \*:\*

UDP 172.20.10.4:138 \*:\*

UDP 172.20.10.4:1900 \*:\*

UDP 172.20.10.4:50478 \*:\*

UDP [::]:123 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:3702 \*:\*

UDP [::]:5353 \*:\*

UDP [::]:5353 \*:\*

UDP [::]:5355 \*:\*

UDP [::]:50072 \*:\*

UDP [::]:50085 \*:\*

UDP [::]:51302 \*:\*

UDP [::]:57203 \*:\*

UDP [::]:57843 \*:\*

UDP [::1]:1900 \*:\*

UDP [::1]:50477 \*:\*

UDP [fe80::de5:6f4e:54a9:1a08%13]:1900 \*:\*

UDP [fe80::de5:6f4e:54a9:1a08%13]:50476 \*:\*

1. Identifier les connexions établies

Lister uniquement les connexions établies sur ta machine.

C:\Windows\system32>netstat -a | find "ESTABLISHED"

TCP 172.20.10.4:50148 172.172.255.217:https ESTABLISHED

TCP 172.20.10.4:50156 20.169.174.231:https ESTABLISHED

TCP 172.20.10.4:50165 13.91.58.244:https ESTABLISHED

TCP 172.20.10.4:50185 4.172.12.147:https ESTABLISHED

TCP 172.20.10.4:50186 52.112.122.33:https ESTABLISHED

TCP 172.20.10.4:50195 104.18.32.47:https ESTABLISHED

TCP 172.20.10.4:50198 52.112.100.56:https ESTABLISHED

TCP 172.20.10.4:50237 52.96.111.98:https ESTABLISHED

TCP 172.20.10.4:50304 52.111.230.4:https ESTABLISHED

TCP 172.20.10.4:50317 52.111.230.4:https ESTABLISHED

TCP 172.20.10.4:50342 172.172.255.218:https ESTABLISHED

TCP 172.20.10.4:50364 13.68.233.9:https ESTABLISHED

TCP 172.20.10.4:50365 172.64.155.209:https ESTABLISHED

TCP 172.20.10.4:50366 20.42.73.24:https ESTABLISHED

TCP 172.20.10.4:50367 52.111.229.57:https ESTABLISHED

TCP 172.20.10.4:50368 ec2-3-233-158-24:https ESTABLISHED

1. Identifier les ports en écoute

Voir quels services écoutent les connexions entrantes sur ta machine.

C:\Windows\system32>netstat -a | find "LISTENING"

TCP 0.0.0.0:135 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:445 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:5040 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:5357 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49664 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49665 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49666 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49667 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49668 DESKTOP-P5EIGGR:0 LISTENING

TCP 0.0.0.0:49670 DESKTOP-P5EIGGR:0 LISTENING

TCP 127.0.0.1:8884 DESKTOP-P5EIGGR:0 LISTENING

TCP 172.20.10.4:139 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:135 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:445 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:5357 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49664 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49665 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49666 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49667 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49668 DESKTOP-P5EIGGR:0 LISTENING

TCP [::]:49670 DESKTOP-P5EIGGR:0 LISTENING

TCP [::1]:42050 DESKTOP-P5EIGGR:0 LISTENING

TCP [::1]:49669 DESKTOP-P5EIGGR:0 LISTENING

1. Afficher les connexions avec les noms des processus

Associer les connexions réseau aux processus en cours d’exécution.

* + chrome.exe utilise le port **55023** pour communiquer avec **93.184.216.34** (probablement un site web).
  + firefox.exe utilise le port **54012** pour communiquer avec **Google**.

Les réponses sont données sous la forme ci-dessous, ce qui signifie que :

chrome.exe utilise le port **50543** pour communiquer avec l’adresse **74.121.140.211**.

* + TCP 172.20.10.4:50543 74.121.140.211:https ESTABLISHED  
    [chrome.exe]

C:\Windows\system32>netstat -b

Active Connections

Proto Local Address Foreign Address State

TCP 172.20.10.4:50148 172.172.255.217:https ESTABLISHED

WpnService

[svchost.exe]

TCP 172.20.10.4:50156 20.169.174.231:https ESTABLISHED

[msedge.exe]

TCP 172.20.10.4:50185 4.172.12.147:https ESTABLISHED

[ms-teams.exe]

TCP 172.20.10.4:50186 52.112.122.33:https ESTABLISHED

[ms-teams.exe]

TCP 172.20.10.4:50195 104.18.32.47:https ESTABLISHED

[msedge.exe]

TCP 172.20.10.4:50317 52.111.230.4:https ESTABLISHED

[Winword.exe]

TCP 172.20.10.4:50387 13.91.62.11:https ESTABLISHED

[msedgewebview2.exe]

TCP 172.20.10.4:50440 172.64.155.209:https ESTABLISHED

[msedge.exe]

TCP 172.20.10.4:50443 52.112.100.56:https ESTABLISHED

[msedgewebview2.exe]

TCP 172.20.10.4:50449 20.7.2.167:https ESTABLISHED

[OneDrive.exe]

TCP 172.20.10.4:50456 200.113.232.99:https CLOSE\_WAIT

[WhatsApp.exe]

TCP 172.20.10.4:50465 200.113.232.225:https CLOSE\_WAIT

[WhatsApp.exe]

TCP 172.20.10.4:50467 40.79.173.41:https TIME\_WAIT

TCP 172.20.10.4:50468 a23-4-43-62:http TIME\_WAIT

TCP 172.20.10.4:50469 51.116.253.170:https ESTABLISHED

[msedgewebview2.exe]

TCP 172.20.10.4:50470 51.116.253.170:https ESTABLISHED

[msedgewebview2.exe]

TCP 172.20.10.4:50471 a23-211-118-80:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50473 a104-70-121-185:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50475 52.96.172.114:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50476 52.168.117.168:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50477 40.118.171.167:https ESTABLISHED

[smartscreen.exe]

TCP 172.20.10.4:50478 lga25s74-in-f10:https TIME\_WAIT

TCP 172.20.10.4:50479 lga25s79-in-f3:https TIME\_WAIT

TCP 172.20.10.4:50480 lga25s71-in-f10:https TIME\_WAIT

TCP 172.20.10.4:50482 lga25s71-in-f14:http TIME\_WAIT

TCP 172.20.10.4:50483 bi-in-f84:https TIME\_WAIT

TCP 172.20.10.4:50484 lga25s71-in-f14:http TIME\_WAIT

TCP 172.20.10.4:50487 lga34s36-in-f14:https TIME\_WAIT

TCP 172.20.10.4:50488 13.107.3.254:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50489 lga34s35-in-f10:https TIME\_WAIT

TCP 172.20.10.4:50490 lga25s71-in-f14:https TIME\_WAIT

TCP 172.20.10.4:50491 13.107.6.254:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50492 104.22.44.142:https TIME\_WAIT

TCP 172.20.10.4:50493 172.202.65.254:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50494 204.79.197.222:https ESTABLISHED

[SearchApp.exe]

TCP 172.20.10.4:50495 lga25s74-in-f10:https TIME\_WAIT

TCP 172.20.10.4:50496 bi-in-f188:5228 ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50497 lga34s35-in-f3:https TIME\_WAIT

TCP 172.20.10.4:50500 195-181-163-195:https FIN\_WAIT\_2

[chrome.exe]

TCP 172.20.10.4:50501 lga25s81-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50502 bi-in-f84:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50503 lga34s32-in-f2:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50505 lga34s40-in-f1:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50506 lga25s73-in-f2:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50507 lga34s39-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50508 a6370ebea231e0c9a:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50510 ip-185-184-8-90:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50511 26:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50512 lga25s77-in-f2:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50515 213:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50516 ec2-3-234-192-86:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50517 13.107.42.14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50518 ec2-52-54-61-185:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50519 ny:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50520 104.18.43.206:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50521 ec2-3-218-92-120:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50523 a184-31-53-154:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50524 195-181-163-195:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50525 lga34s37-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50526 ec2-3-214-226-36:https CLOSE\_WAIT

[chrome.exe]

TCP 172.20.10.4:50528 ny:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50530 134:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50531 ec2-3-214-226-36:https CLOSE\_WAIT

[chrome.exe]

TCP 172.20.10.4:50532 ip184:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50533 192.184.68.254:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50534 li1853-172:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50535 213:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50536 199.38.167.131:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50537 199.38.167.131:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50540 151.101.194.49:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50541 130:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50542 n-sysadmin-jumpbox-03:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50543 74.121.140.211:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50544 74.119.117.16:https FIN\_WAIT\_1

[chrome.exe]

TCP 172.20.10.4:50545 199.38.167.131:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50546 li1853-172:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50548 66:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50549 173:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50550 140:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50551 server-18-244-202-104:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50552 lga34s39-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50553 lga34s34-in-f1:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50554 lga25s74-in-f10:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50555 lga25s80-in-f10:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50556 lga34s40-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50557 lga34s37-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50558 bi-in-f84:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50559 lga25s81-in-f14:https ESTABLISHED

[chrome.exe]

TCP 172.20.10.4:50560 lga34s34-in-f3:https ESTABLISHED

[chrome.exe]

1. Afficher les statistiques réseaux

Obtenir des informations sur les paquets envoyés et reçus.

C:\Windows\system32>netstat -s

IPv4 Statistics:

Packets Received = 64228

Received Header Errors = 0

Received Address Errors = 0

Datagrams Forwarded = 0

Unknown Protocols Received = 0

Received Packets Discarded = 489

Received Packets Delivered = 64514

Output Requests = 53944

Routing Discards = 0

Discarded Output Packets = 312

Output Packet No Route = 54

Reassembly Required = 4

Reassembly Successful = 2

Reassembly Failures = 0

Datagrams Successfully Fragmented = 0

Datagrams Failing Fragmentation = 0

Fragments Created = 0

IPv6 Statistics:

Packets Received = 263

Received Header Errors = 0

Received Address Errors = 0

Datagrams Forwarded = 0

Unknown Protocols Received = 4

Received Packets Discarded = 181

Received Packets Delivered = 685

Output Requests = 1047

Routing Discards = 0

Discarded Output Packets = 42

Output Packet No Route = 0

Reassembly Required = 0

Reassembly Successful = 0

Reassembly Failures = 0

Datagrams Successfully Fragmented = 0

Datagrams Failing Fragmentation = 0

Fragments Created = 0

ICMPv4 Statistics:

Received Sent

Messages 47 220

Errors 0 0

Destination Unreachable 47 220

Time Exceeded 0 0

Parameter Problems 0 0

Source Quenches 0 0

Redirects 0 0

Echo Replies 0 0

Echos 0 0

Timestamps 0 0

Timestamp Replies 0 0

Address Masks 0 0

Address Mask Replies 0 0

Router Solicitations 0 0

Router Advertisements 0 0

ICMPv6 Statistics:

Received Sent

Messages 292 97

Errors 0 0

Destination Unreachable 186 5

Packet Too Big 0 0

Time Exceeded 0 0

Parameter Problems 0 0

Echos 0 0

Echo Replies 0 0

MLD Queries 3 0

MLD Reports 45 0

MLD Dones 4 0

Router Solicitations 0 9

Router Advertisements 7 0

Neighbor Solicitations 37 37

Neighbor Advertisements 10 46

Redirects 0 0

Router Renumberings 0 0

TCP Statistics for IPv4:

Active Opens = 1069

Passive Opens = 5

Failed Connection Attempts = 48

Reset Connections = 209

Current Connections = 40

Segments Received = 47846

Segments Sent = 43826

Segments Retransmitted = 1266

TCP Statistics for IPv6:

Active Opens = 20

Passive Opens = 13

Failed Connection Attempts = 7

Reset Connections = 0

Current Connections = 0

Segments Received = 231

Segments Sent = 207

Segments Retransmitted = 24

UDP Statistics for IPv4:

Datagrams Received = 16442

No Ports = 353

Receive Errors = 136

Datagrams Sent = 8263

UDP Statistics for IPv6:

Datagrams Received = 406

No Ports = 0

Receive Errors = 0

Datagrams Sent = 806

1. Afficher la table de routage

Voir les routes utilisées par ton PC pour communiquer avec d’autres réseaux.   
C:\Windows\system32>netstat -r

===========================================================================

Interface List

36...10 65 30 2e e6 28 ......Intel(R) Ethernet Connection (4) I219-LM #2

22...5c 5f 67 02 91 ef ......Microsoft Wi-Fi Direct Virtual Adapter #18

43...5e 5f 67 02 91 ee ......Microsoft Wi-Fi Direct Virtual Adapter #19

13...5c 5f 67 02 91 ee ......Intel(R) Dual Band Wireless-AC 8265 #6

1...........................Software Loopback Interface 1

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.192.1 192.168.192.12 35

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

192.168.192.0 255.255.255.0 On-link 192.168.192.12 291

192.168.192.12 255.255.255.255 On-link 192.168.192.12 291

192.168.192.255 255.255.255.255 On-link 192.168.192.12 291

224.0.0.0 240.0.0.0 On-link 127.0.0.1 331

224.0.0.0 240.0.0.0 On-link 192.168.192.12 291

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 192.168.192.12 291

===========================================================================

Persistent Routes:

None

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 331 ::1/128 On-link

13 51 fdc4:6e33:f8ba:8100::/64 On-link

13 291 fdc4:6e33:f8ba:8100:201f:dc58:2ff2:4433/128

On-link

13 291 fdc4:6e33:f8ba:8100:abb4:ae2d:e7fe:bb1e/128

On-link

13 291 fe80::/64 On-link

13 291 fe80::de5:6f4e:54a9:1a08/128

On-link

1 331 ff00::/8 On-link

13 291 ff00::/8 On-link

===========================================================================

Persistent Routes:

None

1. Actualiser l’affichage en temps réel

Surveiller les connexions réseau en direct (voir les connexions qui s’ouvrent et se ferment en temps réel)

On répète l'affichage toutes les **1 seconde :**  
C:\Windows\system32>netstat -n 1

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.192.12:50691 52.112.122.38:443 ESTABLISHED

TCP 192.168.192.12:50692 4.172.11.173:443 ESTABLISHED

TCP 192.168.192.12:50704 20.169.174.231:443 ESTABLISHED

TCP 192.168.192.12:50707 108.177.12.188:5228 ESTABLISHED

TCP 192.168.192.12:50710 52.112.100.56:443 ESTABLISHED

TCP 192.168.192.12:50718 13.91.58.244:443 ESTABLISHED

TCP 192.168.192.12:50725 172.172.255.216:443 ESTABLISHED

TCP 192.168.192.12:50744 52.111.230.4:443 ESTABLISHED

TCP 192.168.192.12:50826 31.13.67.53:80 TIME\_WAIT

TCP 192.168.192.12:50831 172.64.155.209:443 ESTABLISHED

TCP 192.168.192.12:50832 20.42.73.25:443 ESTABLISHED

TCP 192.168.192.12:50833 52.228.161.161:443 ESTABLISHED

TCP 192.168.192.12:50834 104.18.32.47:443 ESTABLISHED

TCP 192.168.192.12:50835 13.68.233.9:443 TIME\_WAIT

TCP 192.168.192.12:50836 52.109.76.243:443 TIME\_WAIT

TCP 192.168.192.12:50837 52.109.8.36:443 TIME\_WAIT

TCP 192.168.192.12:50838 23.202.74.187:80 ESTABLISHED

TCP 192.168.192.12:50839 150.171.28.12:443 ESTABLISHED

TCP 192.168.192.12:50840 172.172.255.216:443 ESTABLISHED

TCP 192.168.192.12:50841 13.107.42.12:443 ESTABLISHED

TCP 192.168.192.12:50842 150.171.27.11:443 ESTABLISHED

TCP 192.168.192.12:50843 150.171.27.11:443 ESTABLISHED

TCP 192.168.192.12:50844 52.111.229.62:443 ESTABLISHED

TCP 192.168.192.12:50845 13.107.42.12:443 ESTABLISHED

TCP 192.168.192.12:50847 13.69.239.78:443 ESTABLISHED

TCP 192.168.192.12:50848 35.190.80.1:443 ESTABLISHED

TCP 192.168.192.12:50849 31.13.67.53:80 ESTABLISHED

TCP 192.168.192.12:50850 31.13.67.52:443 ESTABLISHED

TCP 192.168.192.12:50851 31.13.67.52:443 ESTABLISHED

TCP 192.168.192.12:50852 200.113.232.99:443 ESTABLISHED

TCP 192.168.192.12:50853 200.113.232.225:443 ESTABLISHED

TCP 192.168.192.12:50854 31.13.65.49:443 ESTABLISHED

TCP 192.168.192.12:50855 13.68.233.9:443 ESTABLISHED

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.192.12:50691 52.112.122.38:443 ESTABLISHED

TCP 192.168.192.12:50692 4.172.11.173:443 ESTABLISHED

TCP 192.168.192.12:50704 20.169.174.231:443 ESTABLISHED

TCP 192.168.192.12:50707 108.177.12.188:5228 ESTABLISHED

TCP 192.168.192.12:50710 52.112.100.56:443 ESTABLISHED

TCP 192.168.192.12:50718 13.91.58.244:443 ESTABLISHED

TCP 192.168.192.12:50725 172.172.255.216:443 ESTABLISHED

TCP 192.168.192.12:50744 52.111.230.4:443 ESTABLISHED

TCP 192.168.192.12:50826 31.13.67.53:80 TIME\_WAIT

TCP 192.168.192.12:50831 172.64.155.209:443 ESTABLISHED

TCP 192.168.192.12:50832 20.42.73.25:443 ESTABLISHED

TCP 192.168.192.12:50833 52.228.161.161:443 ESTABLISHED

TCP 192.168.192.12:50834 104.18.32.47:443 ESTABLISHED

TCP 192.168.192.12:50835 13.68.233.9:443 TIME\_WAIT

TCP 192.168.192.12:50836 52.109.76.243:443 TIME\_WAIT

TCP 192.168.192.12:50837 52.109.8.36:443 TIME\_WAIT

TCP 192.168.192.12:50838 23.202.74.187:80 ESTABLISHED

TCP 192.168.192.12:50839 150.171.28.12:443 ESTABLISHED

TCP 192.168.192.12:50840 172.172.255.216:443 ESTABLISHED

TCP 192.168.192.12:50841 13.107.42.12:443 ESTABLISHED

TCP 192.168.192.12:50842 150.171.27.11:443 ESTABLISHED

TCP 192.168.192.12:50843 150.171.27.11:443 ESTABLISHED

TCP 192.168.192.12:50844 52.111.229.62:443 ESTABLISHED

TCP 192.168.192.12:50845 13.107.42.12:443 ESTABLISHED

TCP 192.168.192.12:50847 13.69.239.78:443 ESTABLISHED

TCP 192.168.192.12:50848 35.190.80.1:443 ESTABLISHED

TCP 192.168.192.12:50849 31.13.67.53:80 ESTABLISHED

TCP 192.168.192.12:50850 31.13.67.52:443 ESTABLISHED

TCP 192.168.192.12:50851 31.13.67.52:443 ESTABLISHED

TCP 192.168.192.12:50852 200.113.232.99:443 ESTABLISHED

TCP 192.168.192.12:50853 200.113.232.225:443 ESTABLISHED

TCP 192.168.192.12:50854 31.13.65.49:443 ESTABLISHED

TCP 192.168.192.12:50855 13.68.233.9:443 ESTABLISHED

1. Lister les connexions réseau et exporter les résultats

Générer un fichier de rapport contenant toutes les connexions actives.

R- C:\Users\Lafleur\Desktop>netstat -an > connexions.txt

1. Trouver la connexion réseau la plus active

Identifier quelle connexion génère le plus de trafic sur ta machine, après les avoir généré dans un fichier

C:\Users\Lafleur\Desktop>netstat -e -s > statistiques\_reseau.txt

-e : affiche les statistiques Ethernet (paquets envoyés/reçus).

-s : affiche les stats par protocole (TCP, UDP...).

> : redirige la sortie dans un fichier texte.

D’après les statistiques, **la connexion réseau la plus active** est celle utilisant le **protocole TCP sur IPv4**.  
TCP/IPv4 :

* Segments reçus : 58 504
* Segments envoyés : 54 348
* Connexions actives actuelles : 26
* Total d’ouvertures de connexions : 1 372

1. Trouver si une machine du réseau envoie trop de requêtes

Identifier un appareil qui effectue trop de connexions simultanées (ex : infection par un botnet).

* + Si le nombre de connexions **est très élevé** (+100), c’est anormal.
  + Vérifie quelles IP sont concernées avec :

PS C:\Users\Lafleur> netstat -an | Select-String ESTABLISHED | ForEach-Object {

>> ($\_ -split '\s+')[-2]

>> } | Group-Object | Sort-Object Count -Descending | Select-Object -First 10

Count Name Group

----- ---- -----

2 104.18.32.47:443 {104.18.32.47:443, 104.18.32.47:443}

1 23.211.118.35:443 {23.211.118.35:443}

1 52.96.109.210:443 {52.96.109.210:443}

1 13.86.221.35:8883 {13.86.221.35:8883}

1 200.113.232.99:443 {200.113.232.99:443}

1 150.171.73.254:443 {150.171.73.254:443}

1 52.123.129.254:443 {52.123.129.254:443}

1 20.42.73.31:443 {20.42.73.31:443}

1 204.79.197.222:443 {204.79.197.222:443}

1 20.169.174.231:443 {20.169.174.231:443}