

Introduccion a las redes (CCNA1)

Comandos netstat para CMD de Windows

Luis Reyes Volquez

Comando netstat

- Se utiliza para ver las conexiones tcp activas.

```
C:\Users>netstat

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    192.168.7.175:49496   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:49577   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:49920   lb-140-82-112-25-iad:https ESTABLISHED
TCP    192.168.7.175:52044   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:53472   172.172.255.218:https ESTABLISHED
TCP    192.168.7.175:53573   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:53759   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:54455   lb-140-82-113-22-iad:https ESTABLISHED
TCP    192.168.7.175:54462   vk-in-f188:5228      ESTABLISHED
TCP    192.168.7.175:55478   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:56635   a23-50-112-33:https   CLOSE_WAIT
TCP    192.168.7.175:59009   cdn-185-199-108-133:https ESTABLISHED
TCP    192.168.7.175:62388   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:64886   RouterAlcarrizos:domain TIME_WAIT
TCP    192.168.7.175:64890   whatsapp-cdn-shv-01-mia3:https ESTABLISHED

C:\Users>
```

Comando netstat -a

- Se utiliza para ver las conexiones tcp activas en modo escucha.

[illegible][illegible]

Comando netstat -s

- Se utiliza para mostrar las métricas de diferentes protocolos.

C:\Users>netstat -s		Estadísticas de IPv4	
Paquetes recibidos	= 182603277	Paquetes recibidos	= 182603277
Errores de encabezado recibidos	= 0	Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 168794816	Errores de dirección recibidos	= 168794816
Datagramas reenviados	= 7398580	Datagramas reenviados	= 7398580
Protocolos desconocidos recibidos	= 0	Protocolos desconocidos recibidos	= 0
Paquetes recibidos descartados	= 5508958	Paquetes recibidos descartados	= 5508958
Paquetes recibidos procesados	= 6174426	Paquetes recibidos procesados	= 6174426
Solicitudes de salida	= 627214	Solicitudes de salida	= 627214
Descartes de enrutamiento	= 0	Descartes de enrutamiento	= 0
Paquetes de salida descartados	= 601	Paquetes de salida descartados	= 601
Paquetes de salida sin ruta	= 72	Paquetes de salida sin ruta	= 72
Reensamblados requeridos	= 32500	Reensamblados requeridos	= 32500
Reensamblados correctos	= 16228	Reensamblados correctos	= 16228
Reensamblados erróneos	= 0	Reensamblados erróneos	= 0
Datagramas correctamente fragmentados	= 0	Datagramas correctamente fragmentados	= 0
Datagramas mal fragmentados	= 0	Datagramas mal fragmentados	= 0
Fragmentos creados	= 0	Fragmentos creados	= 0
Estadísticas de IPv6		Estadísticas de IPv6	
Paquetes recibidos	= 202178	Paquetes recibidos	= 202178
Errores de encabezado recibidos	= 0	Errores de encabezado recibidos	= 0
Errores de dirección recibidos	= 4566	Errores de dirección recibidos	= 4566
Datagramas reenviados	= 0	Datagramas reenviados	= 0
Protocolos desconocidos recibidos	= 12	Protocolos desconocidos recibidos	= 12
Paquetes recibidos descartados	= 45638	Paquetes recibidos descartados	= 45638
Paquetes recibidos procesados	= 179126	Paquetes recibidos procesados	= 179126
Solicitudes de salida	= 31567	Solicitudes de salida	= 31567
Descartes de enrutamiento	= 0	Descartes de enrutamiento	= 0
Paquetes de salida descartados	= 172	Paquetes de salida descartados	= 172
Paquetes de salida sin ruta	= 0	Paquetes de salida sin ruta	= 0
Reensamblados requeridos	= 16	Reensamblados requeridos	= 16
Reensamblados correctos	= 8	Reensamblados correctos	= 8
Reensamblados erróneos	= 0	Reensamblados erróneos	= 0
Datagramas correctamente fragmentados	= 0	Datagramas correctamente fragmentados	= 0
Datagramas mal fragmentados	= 0	Datagramas mal fragmentados	= 0
Fragmentos creados	= 0	Fragmentos creados	= 0
Estadísticas de ICMPv4		Estadísticas de ICMPv4	
Mensajes	489	Recibidos	489
Errores	0	Enviados	747
Destino inaccesible	175		0
Tiempo agotado	0		747
Problemas de parámetros	0		0
Paquetes de control de flujo	0		0
Redirecciones	0		0
Respuestas de eco	0		0
Ecos	72		0
Marcas de tiempo			0
Respuestas de marca de tiempo			0
Máscaras de direcciones	0		0
Máscaras de direcciones respondidas	0		0
Solicitudes de enrutador	0		0
Anuncios de enrutador	242		0
Estadísticas de ICMPv6		Estadísticas de ICMPv6	
Mensajes		Recibidos	1437
Errores		Enviados	1949
Destino inaccesible			0
Paquete demasiado grande	0		138
Tiempo agotado			0
Problemas de parámetros			0
Ecos			0
Respuestas de eco			692
Consultas MLD	0		0
Informes MLD	12		0
Ejecuciones MLD	12		0
Solicitudes de enrutador	0		135
Anuncios de enrutador	35		0
Solicitudes de vecino	283		1193
Anuncios de vecino	333		483
Redirecciones			0
Renumeraciones de enrutador	0		0
Estadísticas de TCP para IPv4		Estadísticas de TCP para IPv4	
Activos abiertos	= 7230	Activos abiertos	= 7230
Pasivos abiertos	= 1	Pasivos abiertos	= 1
Intentos de conexión erróneos	= 196	Intentos de conexión erróneos	= 196
Conexiones restablecidas	= 923	Conexiones restablecidas	= 923
Conexiones actuales	= 5	Conexiones actuales	= 5
Segmentos recibidos	= 467830	Segmentos recibidos	= 467830
Segmentos enviados	= 393600	Segmentos enviados	= 393600
Segmentos retransmitidos	= 2573	Segmentos retransmitidos	= 2573
Estadísticas de TCP para IPv6		Estadísticas de TCP para IPv6	
Activos abiertos	= 174	Activos abiertos	= 174
Pasivos abiertos	= 10	Pasivos abiertos	= 10
Intentos de conexión erróneos	= 1951	Intentos de conexión erróneos	= 1951
Conexiones restablecidas	= 45	Conexiones restablecidas	= 45
Conexiones actuales	= 0	Conexiones actuales	= 0
Segmentos recibidos	= 6687	Segmentos recibidos	= 6687
Segmentos enviados	= 6512	Segmentos enviados	= 6512
Segmentos retransmitidos	= 21	Segmentos retransmitidos	= 21
Estadísticas de UDP para IPv4		Estadísticas de UDP para IPv4	
Datagramas recibidos	= 760982	Datagramas recibidos	= 760982
Sin puerto	= 347001	Sin puerto	= 347001
Errores de recepción	= 4	Errores de recepción	= 4
Datagramas enviados	= 221326	Datagramas enviados	= 221326
Estadísticas de UDP para IPv6		Estadísticas de UDP para IPv6	
Datagramas recibidos	= 288237	Datagramas recibidos	= 288237
Sin puerto	= 34805	Sin puerto	= 34805
Errores de recepción	= 2	Errores de recepción	= 2
Datagramas enviados	= 22282	Datagramas enviados	= 22282

Comando netstat -ano

- Se utiliza para ver el PID.

```
Administrator: Símbolo del sistema

C:\Users>netstat -ano

Conexiones activas

Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:25 0.0.0.0: LISTENING 1452
TCP 0.0.0.0:80 0.0.0.0: LISTENING 4
TCP 0.0.0.0:443 0.0.0.0: LISTENING 7420
TCP 0.0.0.0:8080 0.0.0.0: LISTENING 15836
TCP 0.0.0.0:8081 0.0.0.0: LISTENING 1076
TCP 0.0.0.0:8082 0.0.0.0: LISTENING 708
TCP 0.0.0.0:8083 0.0.0.0: LISTENING 2088
TCP 0.0.0.0:8084 0.0.0.0: LISTENING 2364
TCP 0.0.0.0:8085 0.0.0.0: LISTENING 3532
TCP 0.0.0.0:8086 0.0.0.0: LISTENING 1044
TCP 127.0.0.1:8087 0.0.0.0: LISTENING 4
TCP 192.168.1.10:8088 0.0.0.0: LISTENING 4
TCP 192.168.1.10:8089 172.16.1.13:8089 ESTABLISHED 4216
TCP 192.168.1.10:8090 142.250.190.13:8090 ESTABLISHED 6992
TCP 192.168.1.10:8091 23.128.1.13:8091 TIME_WAIT 0
TCP 192.168.1.10:8092 192.168.1.10:8092 TIME_WAIT 0
TCP 192.168.1.10:8093 192.168.1.10:8093 TIME_WAIT 0
TCP 192.168.1.10:8094 52.97.239.13:8094 ESTABLISHED 17968
TCP 192.168.1.10:8095 74.125.233.18:8095 ESTABLISHED 6992
TCP 192.168.1.10:8096 23.128.1.13:8096 CLOSE_WAIT 8576
TCP 192.168.1.10:8097 57.140.1.13:8097 ESTABLISHED 13396
TCP 192.168.1.10:8098 0.0.0.0: LISTENING 4
TCP 192.168.1.10:8099 0.0.0.0: LISTENING 22348
TCP [::]:8100 [::]:8100 LISTENING 1452
TCP [::]:8101 [::]:8101 LISTENING 4
TCP [::]:8102 [::]:8102 LISTENING 15836
TCP [::]:8103 [::]:8103 LISTENING 1076
TCP [::]:8104 [::]:8104 LISTENING 708
TCP [::]:8105 [::]:8105 LISTENING 2088
TCP [::]:8106 [::]:8106 LISTENING 2364
TCP [::]:8107 [::]:8107 LISTENING 3532
TCP [::]:8108 [::]:8108 LISTENING 1044
TCP [::]:8109 [::]:8109 LISTENING 5932
TCP [::]:8110 [::]:8110 LISTENING 3956
UDP 0.0.0.0:135 0.0.0.0: *:* 10732
UDP 0.0.0.0:136 0.0.0.0: *:* 16764
UDP 0.0.0.0:137 0.0.0.0: *:* 7420
```

```
Administrator: Símbolo del sistema

UDP 0.0.0.0:135 0.0.0.0: *:* 9576
UDP 0.0.0.0:136 0.0.0.0: *:* 20532
UDP 0.0.0.0:137 0.0.0.0: *:* 1304
UDP 0.0.0.0:138 0.0.0.0: *:* 9576
UDP 0.0.0.0:139 0.0.0.0: *:* 1304
UDP 0.0.0.0:140 0.0.0.0: *:* 1304
UDP 0.0.0.0:141 0.0.0.0: *:* 1304
UDP 0.0.0.0:142 0.0.0.0: *:* 17968
UDP 0.0.0.0:143 0.0.0.0: *:* 10732
UDP 0.0.0.0:144 0.0.0.0: *:* 10732
UDP 0.0.0.0:145 0.0.0.0: *:* 10732
UDP 1.1.1.1:146 0.0.0.0: *:* 4184
UDP 127.0.0.1:147 0.0.0.0: *:* 4184
UDP 127.0.0.1:148 0.0.0.0: *:* 3920
UDP 127.0.0.1:149 0.0.0.0: *:* 10732
UDP 192.168.1.10:150 0.0.0.0: *:* 4
UDP 192.168.1.10:151 0.0.0.0: *:* 4
UDP 192.168.1.10:152 0.0.0.0: *:* 4184
UDP 192.168.1.10:153 0.0.0.0: *:* 4184
UDP 192.168.1.10:154 0.0.0.0: *:* 10732
UDP 192.168.1.10:155 0.0.0.0: *:* 10732
UDP 192.168.1.10:156 0.0.0.0: *:* 4
UDP 192.168.1.10:157 0.0.0.0: *:* 4184
UDP 192.168.1.10:158 0.0.0.0: *:* 4184
UDP 192.168.1.10:159 0.0.0.0: *:* 16764
UDP [::]:160 [::]:160 *:* 10732
UDP [::]:161 [::]:161 *:* 1304
UDP [::]:162 [::]:162 *:* 20532
UDP [::]:163 [::]:163 *:* 9576
UDP [::]:164 [::]:164 *:* 9576
UDP [::]:165 [::]:165 *:* 20532
UDP [::]:166 [::]:166 *:* 1304
UDP [::]:167 [::]:167 *:* 1304
UDP [::]:168 [::]:168 *:* 1304
UDP [::]:169 [::]:169 *:* 10732
UDP [::]:170 [::]:170 *:* 10732
UDP [::]:171 [::]:171 *:* 4184
UDP [::]:172 [::]:172 *:* 4184
UDP [::]:173 [::]:173 *:* 10732
UDP [::]:174 [::]:174 *:* 4184
```

Comando netstat -p tcp Comando netstat -p udp

- Se utiliza para filtrar por protocolos.

```
C:\Users>netstat -p tcp

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 192.168.1.2:80 172.16.17.1:https ESTABLISHED
TCP 192.168.1.2:80 vk.com:https ESTABLISHED
TCP 192.168.1.2:7777 Rou...:main TIME_WAIT
TCP 192.168.1.2:4444 20.100.100.1: ESTABLISHED
TCP 192.168.1.2: Rou...:main TIME_WAIT
TCP 192.168.1.2: Rou...:main TIME_WAIT
TCP 192.168.1.2: lb-...:https ESTABLISHED
TCP 192.168.1.2: Rou...:main TIME_WAIT
TCP 192.168.1.2: wha...:mia3:https ESTABLISHED
```

```
C:\Users>netstat -p udp

Conexiones activas

Proto Dirección local Dirección remota Estado

C:\Users>
```

Comando netstat -ano | find "[puerto]"

- Se utiliza para filtrar por protocolos.

```
C:\Users>netstat -ano | find "443"
TCP    192.168.1.2:443    172.16.1.1:443    ESTABLISHED    4216
TCP    192.168.1.2:443    172.16.1.1:443    ESTABLISHED    17968
TCP    192.168.1.2:443    172.16.1.1:443    ESTABLISHED    4012
TCP    192.168.1.2:443    172.16.1.1:443    ESTABLISHED    6992
TCP    192.168.1.2:443    172.16.1.1:443    ESTABLISHED    13396
UDP    0.0.0.0:443        0.0.0.0:443        5
```