

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.

Comando netstat -a | find "LISTEN"

- Se utiliza para ver los puertos en modo escucha.

C:\Users>netstat -a | find "listen"

C:\Users>netstat -a | find "LISTEN"

TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.1	DESKTOP-7L9CESC:0	LISTENING
TCP	0.6	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	0.0.	DESKTOP-7L9CESC:0	LISTENING
TCP	127.	DESKTOP-7L9CESC:0	LISTENING
TCP	192.	DESKTOP-7L9CESC:0	LISTENING
TCP	192.	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::1]	DESKTOP-7L9CESC:0	LISTENING
TCP	[::1]	DESKTOP-7L9CESC:0	LISTENING

Comando netstat -s

- Se utiliza para mostrar las métricas de diferentes protocolos.

C:\Users>netstat -s		
Estadísticas de IPv4		
Paquetes recibidos	= 182603277	
Errores de encabezado recibidos	= 0	
Errores de dirección recibidos	= 168794816	
Datagramas reenviados	= 7398580	
Protocolos desconocidos recibidos	= 0	
Paquetes recibidos descartados	= 5508958	
Paquetes recibidos procesados	= 6174426	
Solicitudes de salida	= 627214	
Descartes de enrutamiento	= 0	
Paquetes de salida descartados	= 601	
Paquetes de salida sin ruta	= 72	
Reensamblados requeridos	= 32500	
Reensamblados correctos	= 16228	
Reensamblados erróneos	= 0	
Datagramas correctamente fragmentados	= 0	
Datagramas mal fragmentados	= 0	
Fragmentos creados	= 0	
Estadísticas de IPv6		
Paquetes recibidos	= 202178	
Errores de encabezado recibidos	= 0	
Errores de dirección recibidos	= 4566	
Datagramas reenviados	= 0	
Protocolos desconocidos recibidos	= 12	
Paquetes recibidos descartados	= 45638	
Paquetes recibidos procesados	= 179126	
Solicitudes de salida	= 31567	
Descartes de enrutamiento	= 0	
Paquetes de salida descartados	= 172	
Paquetes de salida sin ruta	= 0	
Reensamblados requeridos	= 16	
Reensamblados correctos	= 8	
Reensamblados erróneos	= 0	
Datagramas correctamente fragmentados	= 0	
Datagramas mal fragmentados	= 0	
Fragmentos creados	= 0	
Estadísticas ICMPv4		
	Recibidos	Enviados
Mensajes	489	747
Errores	0	0
Destino inaccesible	175	747
Tiempo agotado	0	0
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	0
Respuestas de marca de tiempo	0	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		
	Recibidos	Enviados
Mensajes	1437	1949
Errores	0	0
Destino inaccesible	70	138
Paquete demasiado grande	0	0
Tiempo agotado	0	0
Problemas de parámetros	0	0
Ecos	692	0
Respuestas de eco	0	0
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	0
Renumeraciones de enrutador	0	0
Estadísticas de TCP para IPv4		
Activos abiertos	= 7230	
Pasivos abiertos	= 1	
Intentos de conexión erróneos	= 196	
Conexiones restablecidas	= 923	
Conexiones actuales	= 5	
Segmentos recibidos	= 467830	
Segmentos enviados	= 393600	
Segmentos retransmitidos	= 2573	
Estadísticas de TCP para IPv6		
Activos abiertos	= 174	
Pasivos abiertos	= 10	
Intentos de conexión erróneos	= 1951	
Conexiones restablecidas	= 45	
Conexiones actuales	= 0	
Segmentos recibidos	= 6687	
Segmentos enviados	= 6512	
Segmentos retransmitidos	= 21	
Estadísticas UDP para IPv4		
Datagramas recibidos	= 760982	
Sin puerto	= 347001	
Errores de recepción	= 4	
Datagramas enviados	= 221326	
Estadísticas UDP para IPv6		
Datagramas recibidos	= 288237	
Sin puerto	= 34805	
Errores de recepción	= 2	
Datagramas enviados	= 22282	

Comando netstat –ano

- Se utiliza para ver el PID.

Proto	Dirección local	Dirección remota	Estado	PID
TCP	0.0.0.0:435	*	LISTENING	1452
TCP	0.0.0.0:*	*	LISTENING	4
TCP	0.0.0.0:*	*	LISTENING	7420
TCP	0.0.0.0:937	*	LISTENING	15836
TCP	0.0.0.0:*	*	LISTENING	1076
TCP	0.0.0.0:*	*	LISTENING	708
TCP	0.0.0.0:*	*	LISTENING	2088
TCP	0.0.0.0:*	*	LISTENING	2364
TCP	0.0.0.0:5532	*	LISTENING	3532
TCP	0.0.0.0:6666	*	LISTENING	1044
TCP	127.0.0.1:8	*	LISTENING	4
TCP	192.168.1.100:*	*	LISTENING	4
TCP	192.168.1.100:72	172.16.5.20:43	ESTABLISHED	4216
TCP	192.168.1.100:2	14.24.13.18:*	ESTABLISHED	6992
TCP	192.168.1.7:3	23.24.13.18:*	TIME_WAIT	0
TCP	192.168.1.3:4	192.168.1.1:*	TIME_WAIT	0
TCP	192.168.1.5:5	192.168.1.1:*	TIME_WAIT	0
TCP	192.168.1.75:6	52.168.13.13:*	ESTABLISHED	17968
TCP	192.168.1.5:2	74.168.13.18:*	ESTABLISHED	6992
TCP	192.168.1.5:5	23.168.13.18:*	CLOSE_WAIT	8576
TCP	192.168.1.100:57	57.168.13.18:*	ESTABLISHED	13396
TCP	192.168.1.1:60	0.168.13.18:*	LISTENING	4
TCP	192.168.1.13:4887	0.168.13.18:*	LISTENING	22348
TCP	[::]:*	[::]:*	LISTENING	1452
TCP	[::]:*	[::]:*	LISTENING	4
TCP	[::]:*	[::]:*	LISTENING	15836
TCP	[::]:4	[::]:0	LISTENING	1076
TCP	[::]:*	[::]:*	LISTENING	708
TCP	[::]:*	[::]:*	LISTENING	2088
TCP	[::]:*	[::]:*	LISTENING	2364
TCP	[::]:*	[::]:*	LISTENING	3532
TCP	[::]:*	[::]:*	LISTENING	1044
TCP	[::]:*	[::]:*	LISTENING	5932
TCP	[::]:*	[::]:*	LISTENING	3956
UDP	0.0.0.0:*	*	LISTENING	10732
UDP	0.0.0.0:*	*	LISTENING	16764
UDP	0.0.0.0:*	*	LISTENING	7420

Comando netstat -p tcp Comando netstat -p udp

- Se utiliza para filtrar por protocolos.

Proto	Dirección local		Dirección remota		Estado
TCP	192.168.1.102	:2	172.17.0.1	:443	https ESTABLISHED
TCP	192.168.1.102	:2	vk.com	:443	ESTABLISHED
TCP	192.168.1.102	:7	Rou	:443	main TIME_WAIT
TCP	192.168.1.102	:4	20.	:443	ESTABLISHED
TCP	192.168.1.102	:4	Rou	:443	main TIME_WAIT
TCP	192.168.1.102	:4	Rou	:443	main TIME_WAIT
TCP	192.168.1.102	:4	lb-	:443	https ESTABLISHED
TCP	192.168.1.102	:4	Rou	:443	main TIME_WAIT
TCP	192.168.1.102	:4	wha	:443	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    192.168.1.102      172.217.13.13        ESTABLISHED      4216
TCP    192.168.1.102      172.217.13.13        ESTABLISHED      17968
TCP    192.168.1.102      54.226.132.13       ESTABLISHED      4012
TCP    192.168.1.102      172.217.13.13        ESTABLISHED      6992
TCP    192.168.1.102      54.226.132.13       ESTABLISHED      13396
UDP    0.0.0.0               54.226.132.13       ESTABLISHED      17968
```