Netstat Command Cheatsheet

A comprehensive cheat sheet for the `netstat` command, covering its common options and usage for network troubleshooting and monitoring. This cheat sheet provides quick references for displaying network connections, routing tables, interface statistics, and more.

Basic Netstat Usage

Displaying Active Connections

`netstat`	Shows active connections.
`netstat -a`	Displays all active connections and listening ports.
`netstat -t`	Shows only TCP connections.
`netstat -u`	Shows only UDP connections.
`netstat -x`	Displays UNIX domain sockets.
`netstat -at`	Displays all TCP connections, including listening sockets.

Displaying Network Interfaces

`netstat -i`	Shows the network interfaces and their statistics.
`netstat -ie`	Displays extended network interface information.
`netstat -in`	Shows numeric network addresses instead of resolving hostnames.
`netstat -c`	Continuously display network statistics, updating every second.

Displaying Routing Table

`netstat -r`	Shows the kernel routing table.
`netstat -rn`	Displays the routing table numerically.
`netstat -route`	Alternative to `netstat -r`.

Advanced Netstat Options

Combining Options

`netstat -ant`	Shows all TCP connections with numeric addresses.
`netstat -anp`	Displays all connections and listening ports with the associated PID and program name (requires sudo).
`sudo netstat -plntu`	Listens for TCP and UDP ports with PID and program name.
`sudo netstat -tulpn`	Shows all listening TCP and UDP ports with PID and program name.

Filtering Connections

`netstat -an | grep :80`	Shows connections on port 80 (HTTP).
`netstat -an | grep :443`	Shows connections on port 443 (HTTPS).
`netstat -an | grep ESTABLISHED`	Shows established connections.
`netstat -an | grep 192.168.1.100`	Shows connections to/from the IP address 192.168.1.100.

Displaying Multicast Group Memberships

`netstat -g`	Shows multicast group memberships.

Netstat Output Interpretation

Connection States

ESTABLISHED: The socket has an established connection.
LISTEN: The socket is listening for incoming connections.
SYN_SENT: The socket is actively trying to establish a connection.
SYN_RECV: A connection request has been received; the socket is waiting to complete the connection.
CLOSE_WAIT: The remote end has shut down; waiting for the socket to close.
LAST_ACK: The remote end has shut down, and the socket is closed. Waiting for acknowledgement.
TIME_WAIT: The socket is waiting after close to handle packets still in the network.
CLOSED: The socket is not in use.

Column Descriptions

Proto: The protocol used (TCP, UDP, etc.).
Local Address: The IP address and port number of the local end of the connection.
Foreign Address: The IP address and port number of the remote end of the connection.
State: The state of the connection (see Connection States above).
PID/Program name: The process ID and name of the program using the socket (requires sudo).

Numeric vs. Symbolic Addresses

By default, `netstat` attempts to resolve IP addresses to hostnames and port numbers to service names. This can be slow if DNS is not configured correctly or if there are many connections.

Using the `-n` option forces `netstat` to display numeric addresses and port numbers, which can be much faster.

Netstat Examples

Troubleshooting Network Issues

To identify which process is listening on a specific port (e.g., port 80):

```
sudo netstat -tulpn | grep :80
```

To check the number of established connections to a web server:

```
netstat -an | grep :80 | grep
ESTABLISHED | wc -l
```

Monitoring Network Traffic

To continuously monitor network interface statistics:

```
netstat -ic 1
```

(This command updates the interface statistics every 1 second.)
To display the routing table and identify the default gateway:

```
netstat -rn
```

Replacing Netstat (Alternatives)

`netstat` is deprecated in favor of `ss` (socket statistics) and `ip` commands. Here are some common replacements:

- **netstat -an | grep :80** can be replaced by: **ss -tln | grep :80**
- **netstat -rn** can be replaced by: **ip route show**
- **netstat -i** can be replaced by: **ip -s link**