ss Cheatsheet

By Dejan Panovski • Updated on May 21, 2026 • Download PDF

Quick reference for listing sockets, listening ports, connection states, and process owners with the ss command

The `ss` command displays socket statistics on Linux and is the modern replacement for `netstat`. This cheatsheet covers the most useful `ss` flags, state and address filters, and common troubleshooting patterns.

Basic Syntax

Core `ss` command forms and output controls.

`ss`	Show non-listening sockets with an established connection
`ss -a`	Show all sockets, listening and non-listening
`ss -n`	Show numeric addresses and ports, no name resolution
`ss -p`	Show the process that owns each socket
`ss -s`	Show a summary of socket counts by type and state

Filter by Protocol

Restrict output to a single socket family.

`ss -t`	TCP sockets
`ss -u`	UDP sockets
`ss -x`	Unix domain sockets
`ss -ta`	All TCP sockets, including listening
`ss -4`	IPv4 sockets only
`ss -6`	IPv6 sockets only

Listening Ports

Find services that are accepting connections.

`ss -l`	Show listening sockets only
`ss -tl`	Listening TCP sockets
`ss -ul`	Listening UDP sockets
`ss -tulpn`	Listening TCP/UDP with process and numeric output
`sudo ss -tlpn 'sport = :80'`	Find the process listening on TCP port 80

Connection State Filters

Narrow output to a specific TCP state.

`ss -tn state ESTABLISHED`	Established TCP connections
`ss -tn state listening`	Listening TCP sockets
`ss -tn state TIME-WAIT`	Connections in `TIME-WAIT`
`ss -tn state CLOSE-WAIT`	Connections in `CLOSE-WAIT`
`ss -tn state ESTABLISHED | tail -n +2 | wc -l`	Count established TCP connections

Address and Port Filters

Match sockets by source or destination.

`ss -tnp 'dport = :443'`	Filter by destination port
`ss -tnp 'sport = :22'`	Filter by source port
`ss -tn dst 192.168.1.5`	Filter by remote address
`ss -tn src 192.168.1.10`	Filter by local address
`sudo ss -tlpn sport = :8080`	Find the process listening on port 8080

Process and Statistics

Tie sockets to processes and read summary counts.

`sudo ss -tp`	TCP sockets with process name and PID
`sudo ss -tulpn`	Listening sockets with owning processes
`ss -s`	Total sockets by transport and state
`ss -tn`	TCP sockets with numeric addresses
`ss -tn dst 203.0.113.10`	All connections to a remote host

netstat to ss Translation

Map old `netstat` commands to their `ss` equivalents.

`netstat -tuln`	`ss -tuln`
`sudo netstat -tulnp`	`sudo ss -tulpn`
`netstat -at`	`ss -ta`
`netstat -ant | grep ESTABLISHED`	`ss -tn state ESTABLISHED`
`netstat -s`	`ss -s`

Troubleshooting

Common `ss` issues and quick fixes.

`-p shows no process`	Run with `sudo` to see sockets owned by other users
`Filters return nothing`	Quote the expression and verify `sport` versus `dport`
`Service names hide ports`	Add `-n` to keep numeric ports
`Output too broad`	Start with `-t`, `-u`, or a `state` filter, then narrow
`Port match too broad`	Use a built-in filter, such as `ss -tlpn 'sport = :80'`

Related Guides

Use these guides for full walkthroughs and related tools.

ss Command in Linux	Full `ss` guide with examples
netstat Command in Linux	The legacy tool `ss` replaces
ip Command in Linux	Modern routes and interface management
How to Check Listening Ports in Linux	Compare `ss`, `netstat`, and `lsof`
lsof Command in Linux	Tie sockets and files back to processes