ss usage:

This section covers ss command usage with examples. The commands might miss some of your favorites so feel free to drop a comment for any addition. ss command gets all of its data from the kernel namespace hence can get more data as compared to netstat.

Common options used with ss command are:

–**n, –numeric** don't resolve service names
-r, –resolve : resolve host hostnames.
-l, –listening display listening sockets
-o, –options show timer information
-e, –extended show detailed socket information
-m, –memory show socket memory usage
-p, –processes show process using socket
–**s, –summar**y show socket usage summary
-N, –net switch to the specified network namespace name
-4, –ipv4 display only IP version 4 sockets
-6, –ipv6 display only IP version 6 sockets
–**0, –packet** display PACKET sockets
-t, –tcp display only TCP sockets
-S, –sctp display only SCTP sockets
-u, –udp display only UDP sockets
-w, –raw display only RAW sockets
-x, –unix display only Unix domain sockets
-f, –family=FAMILY display sockets of type FAMILY

Examples;

List all connections

To list all connections, just execute ss command without any option passed to it.

```
# ss
```

Show all listing tcp sockets including the corresponding process

The option used is **-lt** as described on options list shown previously.

```
# ss -tlp
```

Show all sockets connecting to 192.168.1.10 on port 443

```
# ss -t dst 192.168.1.10:443
```

Show all ssh related connection

```
# ss -t state established '( dport = :ssh or sport = :ssh )'
Recv-Q Send-Q Local Address:Port Peer Address:Port
0 0 192.168.0.16:60334 192.168.20.3:ssh
```

List tcp and udp ports with no hostname resolution

```
# ss -tun
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port
tcp ESTAB 0 0 192.168.0.16:41464 216.58.223.74:443
```

```
tcp ESTAB 0 0 192.168.0.16:57354 5.160.200.106:80
tcp ESTAB 0 0 192.168.0.16:60334 88.198.68.148:22
....
```

Print process which owns the connection

```
# ss -ltp
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 0.0.0.0:ssh 0.0.0.0:* users:(("sshd",pid=7885,fd=3))
LISTEN 0 64 0.0.0.0:shilp 0.0.0.0:*
LISTEN 0 100 127.0.0.1:18083 0.0.0.0:* users:
(("vboxwebsrv",pid=429,fd=9))
...
```

Show socket usage summary

Pass **-s** option to get a list of socket related stats, **-t** and **-u** can be used to show only tcp or udp stats respectively. The default will show both.

```
# ss -s
Total: 818 (kernel 946)
TCP: 65 (estab 42, closed 3, orphaned 4, synrecv 0, timewait 1/0),
ports 0

Transport Total IP IPv6
* 946 - -
RAW 1 0 1
UDP 14 8 6
TCP 62 56 6
INET 77 64 13
FRAG 0 0 0
```

Show timer information

Timer information can be obtained using -o option.

```
# ss -tn -o
```

Display only raw packets

Use **-w** command option,

```
# ss -w
Recv-Q Send-Q Local Address:Port Peer Address:Port
0 0 *:ipv6-icmp *:*
```

If you Love what we do, support us by downloading this tutorial as pdf from the link below:

That's the end of netstat vs ss usage guide on Linux, we'll keep updating the list so follow us on twitter and facebook to get latest updates. Support us by downloading this guide as pdf using the link below.