

Keep an Eye on Your Linux Systems with Netstat

Two of the fundamental aspects of Linux system security and troubleshooting are knowing what services are running, and what connections and services are available. We're all familiar with `ps` for viewing active services. `netstat` goes a couple of steps further, and displays all available connections, services, and their status. It shows one type of service that `ps` does not: services run from `inetd` or `xinetd`, because `inetd/xinetd` start them up on demand. If the service is available but not active, such as `telnet`, all you see in `ps` is either `inetd` or `xinetd`:

```
$ ps ax | grep -E 'telnet|inetd'
520 ?    Ss    0:00 /usr/sbin/inetd
```

But `netstat` shows `telnet` sitting idly, waiting for a connection:

```
$ netstat --inet -a | grep telnet
tcp    0    0  *:telnet  *.*    LISTEN
```

This `netstat` invocation shows all activity:

```
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp    0    0  *:telnet  *.*    LISTEN
tcp    0    0  *:ipp     *.*    LISTEN
tcp    0    0  *:smtp    *.*    LISTEN
tcp    0    0  192.168.1.5:32851  nest.anthill.echid:ircd  ESTABLISHED
udp    0    0  *:ipp     *.*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ACC ] STREAM LISTENING 1065 /tmp/ksocket-carla/klaunchertDCh2b.slave-socket
unix 2 [ ACC ] STREAM LISTENING 1002 /tmp/ssh-OoMGfFm666/agent.666
unix 2 [ ACC ] STREAM LISTENING 819 private/smtp
```

Your total output will probably run to a couple hundred lines. (A fun and quick way to count lines of output is `netstat -a | wc -l`.) You can ignore everything under "Active UNIX domain sockets." Those are local inter-process communications, not network connections. To avoid displaying them at all, do this:

```
$ netstat --inet -a
```

This will display only network connections, both listening and established. Already `netstat` has earned its keep- both the `telnet` and `smtp` services are running. This is bad, because I don't want to have either a `telnet` or `smtp` server running on this machine. So now I know I need to turn them off, and re-configure my startup files so they won't start at boot.

How do you know what services you want running? That is a mondo subject for another day, and an important one. For example, if your system has been compromised, this is one place to find evidence of a Trojan horse or other malware phoning home. In this example, `ipp` is Internet Printing Protocol, which belongs to CUPS (Common Unix Printing System.) If you want your printer to work, this needs to be here. The connection on `192.168.1.5:32851` is my active IRC (Internet Relay Chat) connection. Refer to your `/etc/services` file to learn more about TCP and UDP ports, and the services assigned to them. What It Means

"Proto" is short for protocol, which is either TCP or UDP. "Recv-Q" and "Send-Q" mean receiving queue and sending queue. These should always be zero; if they're not you might have a problem. Packets should not be piling up in either queue, except briefly, as this example shows:

```
tcp    0    593  192.168.1.5:34321  venus.euao.com:smtp  ESTABLISHED
```

That happened when I hit the "check mail" button in KMail; a brief queuing of outgoing packets is normal behavior. If the receiving queue is consistently jamming up, you might be experiencing a denial-of-service attack. If the sending queue does not clear quickly, you might have an application that is sending them out too fast, or the receiver cannot accept them quickly enough.

"Local address" is either your IP and port number, or IP and the name of a service. "Foreign address" is the hostname and service you are connected to. The asterisk is a placeholder for IP addresses, which of course cannot be known until a remote host connects. "State" is the current status of the connection. Any TCP state can be displayed here, but these three are the ones you want to see:

LISTEN- waiting to receive a connection

ESTABLISHED- a connection is active

TIME_WAIT- a recently terminated connection; this should last only a minute or two, then change back to LISTEN. The socket pair cannot be re-used as long the TIME_WAIT state persists.

UDP is stateless, so the "State" column is always blank.

A socket pair is both sides of a TCP/IP connection, like this example for a locally-attached printer:

```
localhost:ipp    localhost:34493    ESTABLISHED
```

Or a telnet connection to a remote server:

```
192.168.1.5:34437    65.106.57.106.pt:telnet    ESTABLISHED
```

A socket is any hostname-port combination, or IP address-port. Continuous Capture

Because all these things change often, how do you capture the changes? Run netstat continuously with the -c flag and record the output:

```
$ netstat --inet -a -c > netstat.txt
```

Then check email, start and stop services, surf the web, log in to a telnet BBS and play Legend of the Red Dragon; then review your capture file to see what it all looks like. Broken DNS

If netstat is taking too long, or not resolving a hostname at all, give it the -n flag to turn off DNS lookups:

```
$ netstat --inet -an Checking Interfaces
```

netstat can help diagnose NIC problems. Use the -i flag when you're troubleshooting a flakey connection, and you suspect your NIC: \$ netstat -i Kernel Interface table

Iface	MTU	Met	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
eth0	1500	0	28698	0	0	0	33742	0	0	0	BMRU
lo	16436	0	14	0	0	0	14	0	0	0	LRU

lo 16436 0 14 0 0 0 14 0 0 0 LRU You should see large numbers in the RX-OK

(received OK) and TX-OK (transmitted OK) columns, and very low numbers in all the others. If you are seeing a lot of RX-ERRs or TX-ERRs, suspect the NIC or the patch cable. This is what the flags mean:

B = broadcast address

L = loopback device

M = promiscuous mode

R = interface is running

U = interface is up