Using netstat

Just typing netstat should display a long list of information that's usually more than you want to go through at any given time.

The trick to keeping the information useful is knowing what you're looking for and how to tell netstat to only display that information.

For example, if you only want to see TCP connections, use netstat --tcp.

This shows a list of TCP connections to and from your machine. The following example shows connections to our machine on ports 993 (imaps), 143 (imap), 110 (pop3), 25 (smtp), and 22 (ssh).It also shows a connection from our machine to a remote machine on port 389 (ldap).

Note: To speed things up you can use the --numeric option to avoid having to do name resolution on addresses and display the IP only.

Code Listing 1: netstat --tcp

```
% netstat --tcp --numeric
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.128.152:993      192.168.128.120:3853    ESTABLISHED
tcp        0      0 192.168.128.152:143      192.168.128.194:3076    ESTABLISHED
tcp        0      0 192.168.128.152:45771    192.168.128.34:389         TIME_WAIT
tcp        0      0 192.168.128.152:110      192.168.33.123:3521        TIME_WAIT
tcp        0      0 192.168.128.152:25       192.168.231.27:44221       TIME_WAIT
tcp        0    256 192.168.128.152:22     192.168.128.78:47258    ESTABLISHED
```

If you want to see what (TCP) ports your machine is listening on, use netstat --tcp --listening. Another useful flag to add to this is --programs which indicates which process is listening on the specified port.

The following example shows a machine listening on ports 80 (www), 443 (https), 22 (ssh), and 25 (smtp);

Code Listing 2: netstat --tcp --listening --programs

```
# sudo netstat --tcp --listening --programs
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address    State       PID/Program name
tcp        0      0 *:www              *:*                LISTEN      28826/apache2
tcp        0      0 *:ssh              *:*                LISTEN       26604/sshd
tcp        0      0 *:smtp              *:*                 LISTEN        6836/
tcp        0      0 *:https        *:*              LISTEN    28826/apache2
```

Note: Using --all displays both connections and listening ports.

The next example uses netstat --route to display the routing table. For most people, this will show one IP and and the gateway address but if you have more than one interface or have multiple IPs assigned to an interface, this command can help troubleshoot network routing problems.

Code Listing 3: netstat --route

```
% netstat --route
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
0.0.0.0	192.168.1.1	0.0.0.0	UG	1	0	0 eth0

The last example of netstat uses the --statistics flag to display networking statistics. Using this flag by itself displays all IP, TCP, UDP, and ICMP connection statistics.

To just show some basic information. For example purposes, only the output from --raw is displayed here.

Combined with the uptime command, this can be used to get an overview of how much traffic your machine is handling on a daily basis.

Code Listing 4: netstat --statistics --route

```
% netstat --statistics --raw
Ip:
    620516640 total packets received
    0 forwarded
    0 incoming packets discarded
    615716262 incoming packets delivered
    699594782 requests sent out
    5 fragments dropped after timeout
    3463529 reassemblies required
    636730 packets reassembled ok
    5 packet reassembles failed
    310797 fragments created
// ICMP statistics truncated
```

Note: For verbosity, the long names for the various flags were given. Most can be abbreviated to avoid excessive typing (e.g. netstat -tn, netstat -tlp, netstat -r, and netstat -sw).

While netstat is a common utility, hopefully this has demonstrated some different ways to make use of the command. For more information see man 8 netstat.

From http://www.gentoo.org/news/en/gwn/20030929-newsletter.xml

image:rdf newsfeed / //static.linuxhowtos.org/data/rdf.png (null)
|
image:rss newsfeed / //static.linuxhowtos.org/data/rss.png (null)
|
image:Atom newsfeed / //static.linuxhowtos.org/data/atom.png (null)
- Powered by
image:LeopardCMS / //static.linuxhowtos.org/data/leopardcms.png (null)
- Running on
image:Gentoo / //static.linuxhowtos.org/data/gentoo.png (null)
-
Copyright 2004-2020 Sascha Nitsch Unternehmensberatung GmbH
image:Valid XHTML1.1 / //static.linuxhowtos.org/data/xhtml.png (null)
:
image:Valid CSS / //static.linuxhowtos.org/data/css.png (null)

:
image:buttonmaker / //static.linuxhowtos.org/data/buttonmaker.png (null)

- Level Triple-A Conformance to Web Content Accessibility Guidelines 1.0 -
- Copyright and legal notices -
Time to create this page: ms
<!--
image:system status display / /status/output.jpg (null)
-->