Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

dnstop: Monitor BIND DNS Server (DNS Network Traffic) From a Shell Prompt

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I monitor my Bind 9 named (or any other dns server) server traffic / network traffic under Linux? How do I find out and view current DNS queries such as A, MX, PTR and so on in real time? How do I find out who is querying my DNS server or specific domain or specific dns client IP address?

A. Log file can give out required information but dnstop is just like top command for monitoring dns traffic. It is a small tool to listen on device or to parse the file savefile and collect and print statistics on the local network's DNS traffic. You must have read access to /dev/bpf*. bpf (Berkeley Packet Filter) which provides a raw interface to data link layers in a protocol independent fashion. All packets on the network, even those destined for other hosts, are accessible through this mechanism. [1]

dnstop can either read packets from the live capture device, or from a tcpdump savefile.

Install dnstop

Type the following command to install dnstop under Debian / Ubuntu Linux:

```
$ sudo apt-get update
$ sudo apt-get install dnstop
```

A note about Red Hat / CentOS / RHEL / Fedora Linux

Install latest version using make command (see below for for binary RPM file). First, grab latest source code by visiting official dnstop website [2].

First install required development libs, enter:

```
# yum install libpcap-devel ncurses-devel
```

Now, grab latest source code using wget command [3], enter:

```
# cd /tmp
# wget http://dns.measurement-factory.com/tools/dnstop/src/dnstop-20080502.tar.gz
# tar -zxvf dnstop-20080502.tar.gz
# cd dnstop-20080502
```

Compile and install dnstop, enter:

```
# ./configure
# make
# make install
```

dnstop rpm file

Alternatively, you can download dnstop rpm from dag's repo for RHEL / CentOS / Fedora Linux [4].

dnstop under FreeBSD

If you are using FreeBSD, follow these installation instructions [5].

Monitor Dns Server

You can monitor various dns data and queries using command line options.

How do I view dns traffic with dnstop?

Simply, type the following command at a shell prompt to monitor traffic for eth0 interface:

```
# dnstop {interface-name}
# dnstop eth0
# dnstop em0
```

Sample output:

```
2 new queries, 220 total queries                 Mon Aug  4 05:56:50 2008

Sources              count      %
---------------- --------- ------
180.248.xxx.26          72   32.7
77.89.xx.108             7    3.2
186.xxx.13.108           5    2.3
90.xxx.94.39             4    1.8
178.xx.77.83             4    1.8
187.xxx.149.23           4    1.8
xxx.13.249.70            4    1.8
1.xxx.169.102            4    1.8
189.xx.191.126           4    1.8
xxx.239.194.97           3    1.4
```

You can force dnstop to keep counts on names up to level domain name levels by using the -l {level} option. For example, with -l 2 (the default), dnstop will keep two tables: one with top-level domain names (such as .com, .org, .biz etc), and another with second level domain names (such as co.in, col.uk).

```
# dnstop -l 3 eth0
```

Under Debian / Ubuntu Linux, enter:

```
# dnstop -t -s eth0
```

Where,

- -s Track second level domains
- -t Track third level domains

Please note that increasing the level provides more details, but also requires more memory and CPU to keep track of DNS traffic.

How do I exit or reset counters?

To exit the dnstop, hit ^X (hold [CTRL] key and press X). Press ^R to reset the counters.

How do find out TLD generating maximum traffic?

While running dnstop, hit 1 key to view first level query names (TLDs):

```
5 new queries, 1525 total queries                Mon Aug  4 06:11:09 2008

TLD                                 count      %
------------------------------ --------- ------
net                                   520   34.1
biz                                   502   32.9
in-addr.arpa                          454   29.8
in                                     23    1.5
org                                    15    1.0
com                                    11    0.7
```

Look like this DNS server is serving more .net TLDs. You can also find out more about actual domain name by hinting 2 key while running dnstop:

```
3 new queries, 1640 total queries                Mon Aug  4 06:13:20 2008
```

```
SLD                              count      %
------------------------------ --------- ------
cyberciti.biz                      557   34.0
nixcraft.net                       556   33.9
74.in-addr.arpa                     34    2.1
208.in-addr.arpa                    29    1.8
195.in-addr.arpa                    28    1.7
192.in-addr.arpa                    27    1.6
64.in-addr.arpa                     27    1.6
theos.in                            23    1.4
203.in-addr.arpa                    20    1.2
202.in-addr.arpa                    18    1.1
212.in-addr.arpa                    15    0.9
nixcraft.com                        13    0.8
217.in-addr.arpa                    13    0.8
213.in-addr.arpa                    12    0.7
128.in-addr.arpa                    12    0.7
193.in-addr.arpa                    12    0.7
simplyguide.org                     12    0.7
cricketnow.in                        3    0.2
```

To find out 3 level domain, hit **3** key:

```
www.cyberciti.biz         60   39.0
figs.cyberciti.biz        33   21.4
ns1.nixcraft.net          18   11.7
ns3.nixcraft.net          13    8.4
ns2.nixcraft.net          13    8.4
theos.in                   5    3.2
nixcraft.com               5    3.2
cyberciti.biz              2    1.3
jobs.cyberciti.biz         1    0.6
bash.cyberciti.biz         1    0.6
```

How do I display the breakdown of query types seen?

You can easily find out most requested, query type (A, AAAA, PTR etc) by hinting **t** key

```
Query Type     Count      %
---------- --------- ------
A?               224   56.7
AAAA?            142   35.9
A6?               29    7.3
```

How do I find out who is connecting to my DNS server?

Hit d to view dns client IP address:

```
Source         Query Name        Count       %
-------------- ------------ ---------  ------
xx.75.164.90   nixcraft.net          20    9.1
xx.75.164.90   cyberciti.biz         18    9.1
x.68.25.4      nixcraft.net           9    9.1
xxx.131.0.10   cyberciti.biz          5    4.5
xx.104.200.202 cyberciti.biz          4    4.5
202.xxx.0.2    cyberciti.biz          1    4.5
```

Option help

There many more option to provide detailed view of current, traffic, just type **?** to view help for all run time options:

```
 s - Sources list
 d - Destinations list
 t - Query types
 o - Opcodes
 r - Rcodes
```

```
  1 - 1st level Query Names      ! - with Sources
  2 - 2nd level Query Names      @ - with Sources
  3 - 3rd level Query Names      # - with Sources
  4 - 4th level Query Names      $ - with Sources
  5 - 5th level Query Names      % - with Sources
  6 - 6th level Query Names      ^ - with Sources
  7 - 7th level Query Names      & - with Sources
  8 - 8th level Query Names      * - with Sources
  9 - 9th level Query Names      ( - with Sources
^R - Reset counters
^X - Exit

  ? - this
```

Further readings:

- man dnstop
- dnstop project home page

Updated for accuracy.