# Table Of Contents

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

Home > Faq > AIX

# TCPDump: Capture and Record Specific Protocols / Port

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I capture specific protocol or port such as 80 ( http ) using TCPDump tool under Linux / UNIX? How do I recording Traffic with TCPDump and find problems later on?

[1]

A. TCPDump is a tool for network monitoring and data acquisition. It can save lots of time and can be used for debugging network or server related problems. Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression.

## Monitor all packets on eth1 interface

```
tcpdump -i eth1
```

## Monitor all traffic on port 80 ( HTTP )

```
tcpdump -i eth1 'port 80'
```

## Monitor all traffic on port 25 ( SMTP )

```
tcpdump -vv -x -X -s 1500 -i eth1 'port 25'
```

Where,

- **-vv** : More verbose output
- **-x** : When parsing and printing, in addition to printing the headers of each packet, print the data of each packet.
- **-X** : hen parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols.
- **-s 1500**: Snarf snaplen bytes of data from each packet rather than the default of 68. This is useful to see lots of information.
- **-i eth1** : Monitor eth1 interface

## Capturing traffic information using cronjobs

tcpdump can be used to find out about attacks and other problems. Let us say your webserver facing problem everday at midnight. Enter following command into cron. It will schedule [2] capturing of 30,000 packets and writing raw data to a file called port.80.debug.txt:

```
@midnight /usr/sbin/tcpdump -n -c 30000 -w /root/port.80.debug.txt
```

Next day you can log into your box and read the /root/port.80.debug.txt file:

```
tcpdump -X -vv -r /root/port.80.debug.txt
```

This simple technique can be used record and debug problems.

### Further readings:

- man page tcpdump

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/tcpdump-capture-record-protocols-port/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/unix/**
[2] into cron. It will schedule: **http://www.cyberciti.biz/faq/how-do-i-add-jobs-to-cron-under-linux-or-unix-oses/**