


NTOP NET VALUE

CHRISTIAN PERLE



The increasingly networked world of computers is now marching into the living room. The second or third machine is linked with the main home PC and happily swaps data via **TCP/IP**. If you want to keep on top of your private computer farm and its outward network connections, you will find *ntop* by Luca Deri very handy.

Top N

To run the program, the *ncurses* **library** (including associated **Development Packet**) must be installed. You'll also need *libpcap*. To compile the *libpcap* you will need the packages *flex* and *bison*. Ntop can be obtained at www.ntop.org/ntop.html.



Figure 1:
ntop in the text terminal

TCPIP: "Transmission Control Protocol/Internet Protocol", the network **protocol** family of the Internet.

Protocol: A standardised language, with which programs understand each other.

library: files containing a collection of useful C functions for specific purposes. So there are such things as *libm*, which provides mathematical functions, or the *libpcap*, which can tap and examine network packets. Often, libraries are used by several programs (shared).

Development packet: When compiling source texts you will need the development packets for all the libraries used by the program. The header files are an essential component (ending in *.h*), which specify the parameters of the functions included in the libraries.

Compile: A program in source text form from a higher programming language cannot be executed by the operating system as it is. It is only by compiling (translating) it with a Compiler that it is converted into a form which the respective processor can execute.

Throughput: The throughput states how much data per unit of time (usually measured in KBit/second or MBit/second) is passing via a network device.

Man page: The man pages (short for "Manual pages") are an online reference manual for UNIX commands. These are called up with *man* command.

Port: A docking point for network connections. Ports are given numbers, and many are assigned to a service via this number. For example *FTP* uses Port 21, *SSH* Port 22, *TALK* Port 517, etc.

Home-directory: The personal home directory of a user. This is the first directory after successfully logging on or with the command *cd* (without additional parameters).

Out of the Box takes the pick of the bunch of the thousands of utilities available and suggests programs that are indispensable or unduly ignored. This month is devoted to network monitor *ntop*.

Ntop can be **compiled** and installed with:

```
tar xzf libpcap-0.6.2.tar.gz
cd libpcap-0.6.2
./configure --prefix=../libpcap
make
make install
cd ..
tar xzf ntop-1.1-src.tgz
cd ntop-1.1
./configure
make
su (enter root password)
cp ntop /usr/local/bin
cp ntop.8 /usr/local/man/man8
exit
```

SUID or not SUID?

ntop has to run with *root* rights. You can obtain the necessary rights with the *su* command (and *root* password), before you start *ntop*, and give them up again after closing down the program with *exit*.

Alternatively, you can issue (as *root*) with *chmod 4755 /usr/local/bin/ntop* the SUID ("Set UserID on execution") right. So *ntop* - regardless which user has started it - will always run with *root* rights.

The first option is more secure, because then only users who know the *root* password are allowed to monitor the Net. A better, more controlled assignment of *root* rights to users is offered by the program *sudo*.

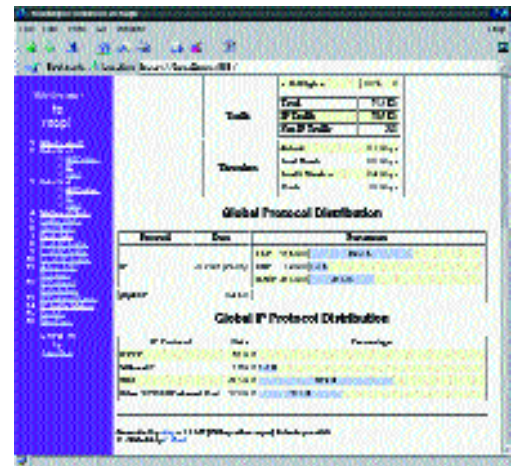


Figure 2: Statistics in the Web interface

If *ntop* is started in a terminal it behaves similar to the UNIX classic *top*, except that *ntop* does not display the processor capacity being used by various processes, but the network traffic due to various computers. In Figure 1 a large movement of data is taking place, from *sphere* to *camera*. The current **throughput** can be read off at top right. The program started with *ntop -i eth0*, thus instructed also to tap packets on the first Ethernet card.

In the text interface *ntop* responds to various keys. The space bar fetches additional information into the columns of the displayed table, such as protocols like FTP, HTTP or DNS. Other functions can be found on the **Man page**.

We shall now leave the text interface with the *q* key and start the program again with *ntop -i eth0 -w 888*. The terminal shows no output, but with a frame-capable web browser you can connect to **Port 888** with the *ntop* service thus started. This is done by entering *http://localhost:888/* as the site

address. You must send a Ctrl+C into the terminal with the *ntop* command, to shut down the service.

ntop makes more information available via the Web interface. Figures 2 and 3 show just a small selection of the statistics on the distributions of protocols in the total throughput, bandwidth utilisation, network card manufacturer, network connections currently running and much more. In Table 1 all the links from the *ntop* main page and their functions are described.

The Web interface can be blocked by a password.

To do this, the user must make a file in their **home directory** called *.ntop* with a user name/password pair. The content of this file could look something like this:

```
# ntop password file
tux    dryfish
```



Figure 3: Overview of individual computers

Some information on network protocol

Basic Protocols

(R)ARP (“[Reverse] Address Resolution Protocol”) is used to find the MAC address of a network card for an IP address. This is the only way in a local network for IP packets to be sent to the right computer. The MAC (“Media Access Control”) address is an address determined by the hardware of the network card.

IP (“Internet Protocol”) is a transport mechanism for various protocols such as TCP and UDP. It sends packets on the basis of their destination IP address. IP is not restricted to a local network.

TCP (“Transmission Control Protocol”) is a connection-oriented protocol, via which many service protocols such as HTTP, SSH or NBios-IP run. Whilst, with IP, packets are merely sent, TCP offers confirmation of receipt. In this case, connection-oriented means that network connections must be explicitly made and disconnected by special IP packets.

UDP (“User Datagram Protocol”) is a connectionless protocol, via which service protocols such as DNS run. UDP is not suitable for the reliable transfer of large amounts of data. “Connectionless” means that within the protocol there is no option for making sure that a packet has really arrived at the receiver’s end.

A small selection of service protocols

HTTP (“Hypertext Transfer Protocol”) is the transfer protocol used by the World Wide Web.

SSH (“Secure Shell”) is an encrypted protocol for logging on to remote computers.

NBios-IP (“Netbios over IP”, also known as SMB (“Server Message Block”)) is the protocol a Samba server uses for Windows file release?

DNS (“Domain Name Service”) resolves computer names such as *www.linux-magazine.co.uk* into IP addresses.

Table 1: Which link shows what?

No.	Name	Meaning
1.	What’s ntop?	General information about <i>ntop</i> .
2.	Data Rcvd	Summary of received data, broken down into data, allotted to IP or all protocols, together with throughput.
3.	Data Sent	Summary of data sent, broken down into IP, all protocols and throughput.
4.	Multicast Stats	Packets which are sent simultaneously to several computers.
5.	Traffic Stats	Information on packet sizes and distribution of protocols in the total throughput.
6.	Thpt Stats	The throughput for the last 60 minutes as bar graph
7.	Hosts Info	Information on computers, broken down by computer
8.	R->L IP Traffic	Network traffic from outside into the local network
9.	L->R IP Traffic	Network traffic from the local network to the outside
10.	L<->L IP Traffic	Network traffic within the local network
11.	Active TCP Sessions	Currently active TCP connections
12.	IP Protocol Distribution	Distribution of the protocols transported via IP
13.	IP Protocol Usage	Which protocols are used between which computers
14.	IP Traffic Matrix	How much was transferred and between which computers
15.	Credits	Thanks from the author
16.	Man Page	The manual page for <i>ntop</i>