Ntop
Bandwidth Monitoring Guide

[VERSION 1.0]

MUKOM AKONG TAMON

techowto.wordpress.com

Table of Contents

Introduction

Being an Open Source fan, I have always heard of this application called ntop (every serious network guru must have) and I even have used its cousin – top for Linux on a few occasions. I finally got round to giving it a try and was a bit disappointed that such a wonderful tool didn't have a nice Guide which is as elegant as the program itself is. Luca Deri – the program's author has done a wonderful job and so I thought I'd emulate his example and contribute something to the FOSS commonwealth by doing something about documentation to start people off. This document draws heavily from what little info I could glean from the web, ntop forums as well as my own experience installing and using ntop on Ubuntu Server 8.04 in a large university network – Ahmadu Bello University, Zaria in Nigeria.

I have absolutely no experience deploying and using ntop on Windows so most of what is reflected in this guide is related to Linux, particularly Ubuntu. I will upgrade this guide as my knowledge grows and everyone can send me information to be added to it by mailing me – mukom.tamon@gmail.com

Great thanks go Luca Deri, Yuri Francalacci and Ricardo Paterna who looked at my initial mind map and offered suggestions and have offered to help me with answers in updating this guide and making it more accurate.

Fundamental Knowledge

What is ntop and what do You Use it for?

Ntop is a simple, free a portable traffic measurement and monitoring tool, initially conceived by Luca Deri and Stefano Suin at the University of Pisa in Italy. It is known to work under Linux, Mac OS X, FreeBSD, Solaris and 32-bit versions of Windows. Ntop gives you an unprecedented amount of visibility into your network like which hosts are consuming most of your bandwidth (the top talkers), what are the most used protocols and applications on your network. Ntop also drills down even to show which peers a particular host has contacted contacting as well as local host traffic matrix that tells you the amount of information that hosts on your local network are exchanging between themselves. All of this information is very useful for network management and planning. In my case, I always thought I had about 1000 users on my network trying to access the web during peak times. On implementing ntop, I was amazed at how ignorant I was about my network – ntop told me I actually had about 2800 hosts!!!! A caveat though ... to get real visibility into your network, the network must be routed and not using port address translation (PAT) internally. Ntop will see every host behind a PAT router as a single device – albeit with multiple connections from it i.e. PAT generates a shield (think StarTrek) which even ntop can't penetrate.

Ntop is an example of a spot check tool i.e., tools used that give you a quick view of what is happening on your network in real-time. Like me, your first use of ntop would occur when the need for bandwidth management becomes obvious and you need to answer the question – just who exactly is consuming most of our bandwidth, for what purpose (i.e. application) and which sites do they visit? A good network engineer always does analysis and investigation before trying to solve a problem on the network. Ntop can monitor IP, IPX and AppleTalk statistics as well as statistics for Fiberchannel and SCSI – but as we all know, IP rules and so most monitoring will be IP-based. Ntop will measure the following types of traffic:

- ☑ Data sent/received: Volume and packets, classified according to network/IP protocol.
- ☑ Multicast Traffic.
- ☑ TCP Session History.
- ☑ Bandwidth Measurement and Analysis.
- ☑ VLAN and BGP Autonomous System [AS] traffic statistics.

- ☑ VoIP (SIP, Cisco SCCP) Monitoring.

In addition, ntop offers you the following options for traffic monitoring and characterization:

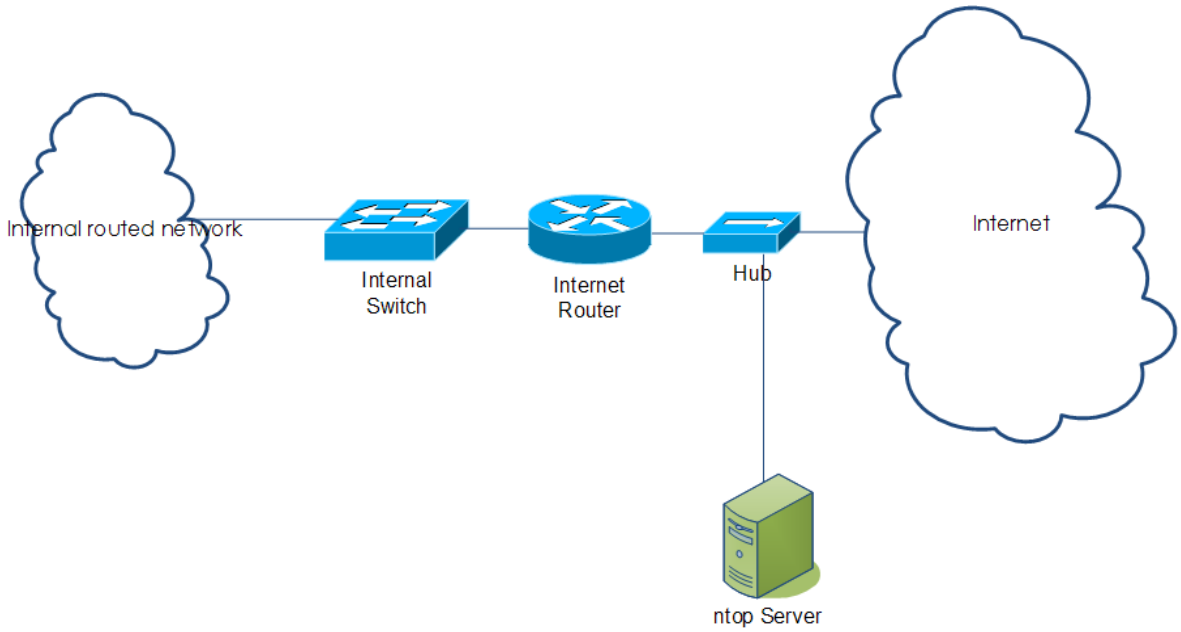
- ☑ Network Flows (user configurable)
- ☑ Protocol utilization (number of requests, peaks/storms, positive/negative replies) and distribution.
- ☑ Network Traffic Matrix.
- ☑ ARP, ICMP Monitoring.
- ☑ Detection of many popular P2P protocols

Ntop data is generally not persistent i.e. it is stored and used from memory and so is lost when the server is rebooted or dumped after a certain time period. In practice, this means that you can't go back and see the analysis for a period prior to the last reboot. By default, you cannot also store the information in a database for later analysis (although there are scripts that will enable you to do that). Ntop can also use Round Robin Databases to store data that is used for graphs and so you can get historical information only for the period of the RRD. There is also a web option that allows us to dump data in XML and other formats for analysis by external tools.

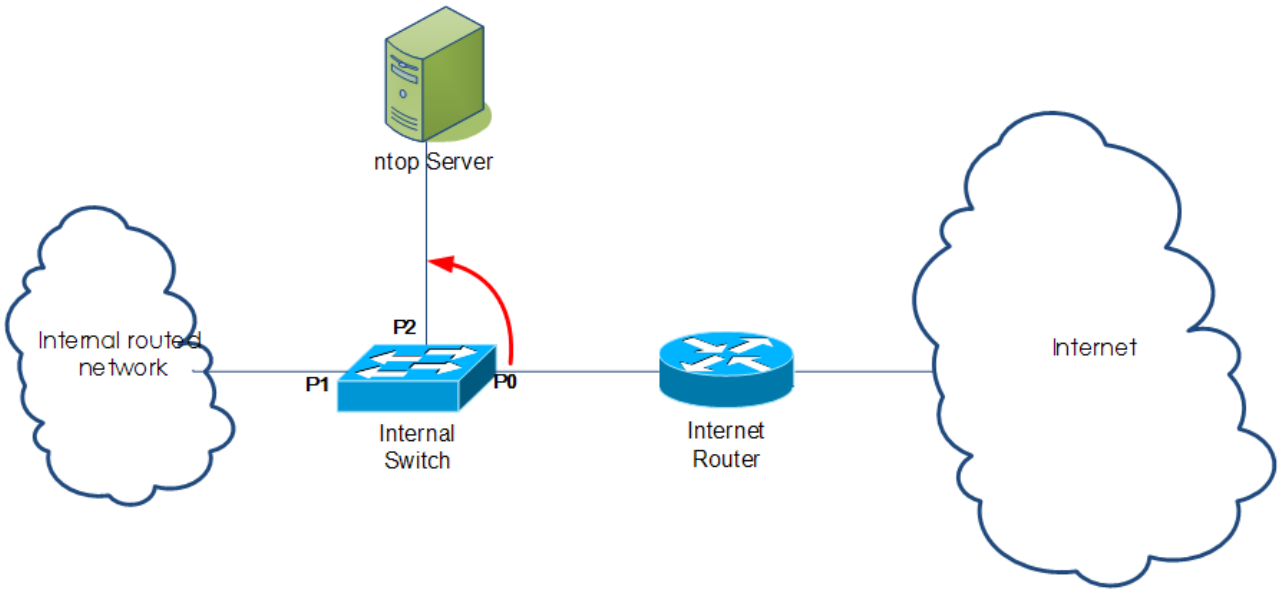
Directing Traffic to ntop [NetFlow vs. SPAN vs. Hub]

Ntop only monitors what it 'sees' from its own physical connection to the network or is 'told' by a NetFlow or sFlow probe or meter. The options for feeding data to ntop are as follows:

a. Use a hub: I know most networks don't use hubs but the property of a hub we are interested in is that unlike a switch, when a frame enters one port of a hub, it is automatically sent out all other ports and so if we plug out Internet connection, internal network and our ntop monitoring server into different ports of a hub, then ntop will see all traffic that is exchanged between our local network and the Internet. No configuration is needed on the hub or switch or router. Except you don't have switches capable of port mirroring, most people will likely never resort to this option so I include it here just for completeness.



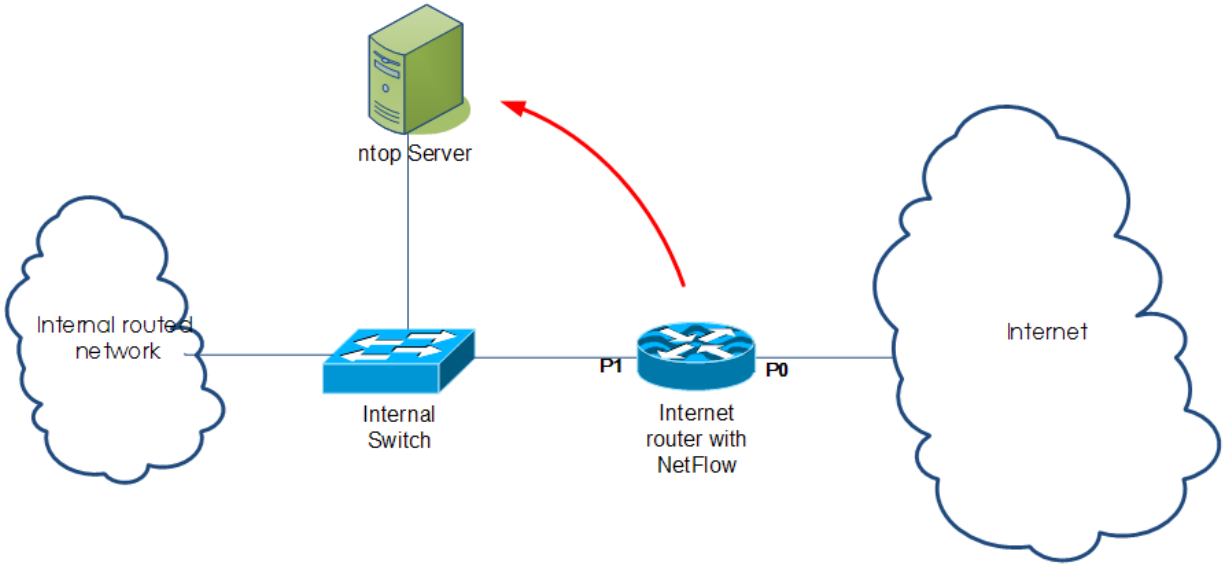
b. Use port mirroring: Unlike hubs, each port of a switch is its own collision domain – meaning that unless a frame is an unknown unicast[1], broadcast or multicast[2], it will only be forwarded out the port where it should go [as determined by the destination MAC address in the frame]. This means that if we replace our hub in the previous scenario with a switch, then the only thing that the ntop server will see are broadcasts, multicasts, unknown unicasts and unicasts that are directed to it. As such, most of the traffic being exchanged between local network and Internet will not be seen and analyzed by ntop. Some switches have a feature that allows the administrator to work round this. Essentially, the administrator can configure the switch such that all traffic that comes in or goes out a set of ports gets also copied and sent to a particular port to which we then plug in our ntop server. Cisco calls this feature SPAN (Switched Port Analyzer) and it works on the majority if not all of Cisco's switches. The most efficient way to capture Internet-related traffic is to mirror both received and transmitted frames on port P0[3] [the switch port connected to the Internet router] to the port on which the ntop server is plugged – P2 in the diagram. Be sure to monitor for whatever port you choose both incoming and outgoing frames. On Cisco switches, you can choose to monitor traffic from several ports [source ports] but beware, the aggregate traffic of multiple source ports may be more than the destination port can handle. Since we are often interested in offsite traffic like Internet traffic, I recommend mirroring only traffic coming in and going out of that single port that which connects to the Internet router [P0 in the diagram].



One caveat to this configuration is that you will need two interfaces on your ntop server. When using Cisco equipment, a port configured as a SPAN destination cannot transmit any traffic except traffic related to the SPAN session. You will thus need another network card through which you can access the ntop machine. This second network card will have the IP address by which the server is identified. The network card connected to the mirrored port really doesn't require an IP address so I just make sure that it comes up during start-up.

[1] Unicast frame for which the switch doesn't have a destination MAC address in its lookup table.
[2] Assuming there are no layer 2 optimizations like IGMP snooping or CGMP on the switch.
[3] Px here is just a generic port representation. On a Cisco switch for example, this will be something like FastEthernet 0/2.

c. Use NetFlow Probes: NetFlow is a Cisco technology that has been adopted by the industry. A NetFlow probe aggregates flows and can send them to a flow collector for analysis. Ntop is a NetFlow collector. I believe that for effectiveness, NetFlow probes should be placed at aggregation points i.e. on the LAN side of all access layer routers or alternatively on the internal interface of the Internet router. The procedures and commands differ for different vendors but essentially you will need to specify the NetFlow version number, the IP address of the NetFlow collector [which in our case is your ntop machine] and the port on which the collector is listening (typically 2055). sFlow is a more standards-compliant alternative to NetFlow which is capable of monitoring gigabit-capable links. Ntop is also a fully capable sFlow collector. Needless to say, the IP address of your ntop machine should be reachable from the NetFlow/sFlow device.



When using the hub or switch-port mirroring options, the network card in the ntop server that listens for traffic needs to be in promiscuous mode i.e. it should process all packets that it sees whether they are destined for it or not. Promiscuous mode is the default mode for the network interfaces on which ntop listens.

Port mirroring may end up giving you the most accurate statistics because ntop gets to actually see the traffic as it flows between systems. With NetFlow/sFlow, only a representation of that traffic is sent to ntop and so features like OS fingerprinting and P2P protocol detection may be inaccurate or not work.

The Effect of Port Address Translation (PAT) on Ntop

With PAT, many devices behind the PAT router take on the IP address of the PAT router albeit from different ports. You are using PAT when you do most forms of Internet Connection Sharing or IP Masquerading.

The problem with PAT from ntop's perspective is that the PAT router modifies a packet from the client and replaces the IP address and source ports of the original packet with its own before sending the packet to its destination. Now if the data that ntop gets to analyze is taken from a segment after this modification, then ntop will only see one host – the PAT router and not all the other hosts 'behind' it.

Most organizations which don't have huge blocks of public IP addresses use PAT at the edge of their networks to allow everyone to access the Internet. So long as the entire internal network is routed and PAT is only done at the edge, then ntop will work fine if the NetFlow probe is configured on the interface of the PAT router that connects to the internal network. For the hub option or SPAN option to work, the ntop server must be in the internal network.

INSTALLING NTOP

Like most other Linux programs, you can install ntop from software repositories of both Debian-based and RPM-based distributions and you can download the sources and compile it yourself. Compiling scares most people but if you compile ntop from source, you can get a version more recent that what is available in repositories. As I write this, the latest stable version of ntop which you can download from sourceforge.net is 3.3.7, while the version of ntop in the repositories is 3.3.2. Also, when you compile, you can tune it very specifically to your needs – that kind of tuning and tweaking is not possible with versions of ntop from the repositories.

INSTALLING FROM SOURCE

The key to a painless source installation is to ensure that all dependencies required by ntop are satisfied. Bottom line is that whenever some dependency is missing, ntop will not compile and will spill an error message to indicate what package it needs to use but can't find. When this happens, one thing to do is to search your repositories for the package that is mentioned in the error message. Another thing I usually do is google that error message and from there I can figure out which packages need to be installed to satisfy that dependency. That said, for first time users, I would advise installing ntop from repositories --- get the thing up and running first. My test system is Ubuntu Server 8.04 with AMP [Apache MySQL & PHP] and OpenSSH servers pre-installed.

1. Download the ntop sources from sourceforge.net. It is usually a gzipped tarball e.g. ntop-3.3.7.tar.gz.
2. Extract the contents of sources from the tarball by typing
   `untar –xzvf ntop-3.3.7.tar.gz`
3. Install all dependencies. [Although listed here as different commands, you could do the same thing with a single command by putting all the packages separated by a space after a single sudo apt-get install command.]

   The list of dependencies required are listed in the following table along with a brief description of what exactly they provide for ntop.

Dependency	Description
glibc, glibc-devel, gcc, cpp	Required to compile almost any software from source.
awk	A utility for performing text-processing tasks.
libtool (1.4 or later)	Required to compile almost any software from source.
m4	Required to compile almost any software from source.
autoconf (2.53 or later)	Required to compile almost any software from source.
automake (1.6 or later)	Required to compile almost any software from source.
gdbm, gdbm-devl	Lightweight alternative to a full relational database. Enables storing and fast lookup with keys of arbitrary data.
libpcap, libpcap-dev	Required to decode the packets that are fed to ntop
gd, gd-dev	Used to create .png picture files
libpng,libpng-dev	Used to create .png picture files
openssl,openssl-dev	Enables access to ntop web UI via https
zlib,zlib-dev	Used to compress HTML pages
rrdtool, librrd2, librrd2-dev	Used to create 'Round-Robin databases' which are used to store and graph historical data in a format that permits long duration retention without growing larger over time.
graphviz	Used to construct the local traffic map [It provides the **dot** tool]

Now, on to the commands (valid for all Debian-based Linux distributions)

```
sudo apt-get install build-essential[4]
sudo apt-get install libtool
sudo apt-get install autoconf
sudo apt-get install automake
sudo apt-get install m4
sudo apt-get install libpcap
sudo apt-get install libpcap-dev
sudo apt-get install libgdbm-dev
sudo apt-get install zlib1g
sudo apt-get install zlib1g-dev
sudo apt-get install rrdtool
sudo apt-get install librrd2
sudo apt-get install librrd2-dev
sudo apt-get install graphviz
```

4. Change into the sources directory created when you extracted the source tarball [`cd ntop-3.3.7`]
5. Compile and install the application by typing each of the following individually and waiting for it to complete without any errors.

```
./autogen.sh
make
sudo make install
```

Look in the output of the commands for any error messages. Error messages in the ./autogen.sh command are most likely due to unmet dependencies. One way to troubleshoot is google the exact text in the error message. Chances are someone else has run into the particular problem, posted it on the mailing list and gotten an answer.

Ntop needs to be started with root privileges in order that it may capture packets from the network cards in the machine. But soon after starting, by default, it will drop privileges to the user called nobody [unless you explicitly specified another user with the –u option]. The important thing to note is that the user to which ntop drops privileges must have appropriate rights in the location where ntop stores its databases (which is /usr/local/var/ntop by default). To set the ownership and rights on that directory, type `chown –R /usr/local/var/ntop`

To set the admin password, type `sudo ntop –A`[5] then fill in and confirm your ntop admin password.

Now run ntop by typing `sudo ntop –d` [the –d option daemonizes ntop so it runs in the background]. Also note that ntop needs to be started with root privileges in order for it to put an interface in promiscuous mode. To make it run at start-up and listen on the first network interface, insert `sudo /usr/local/bin/ntop -d` in /etc/rc.local. I am sure there are other more elegant ways but that is what worked for me when I compiled from sources. If you understand System V scripts very well, you may be able to achieve the same results.

[4]Build-essential is a meta package that contains dpkg-dev, package building tools for Debian, g++ (>= 4:4.1.1) - the GNU C++ compiler , gcc (>= 4:4.1.1) - the GNU C compiler , libc6-dev – the GNU C Library: Development Libraries and Header Files or libc-dev – a virtual package provided by libc6-dev , as well as make - the GNU version of the "make" utility.

[5] During my installation, when I ran this command, I got the error message: `"/usr/local/bin/ntop: error while loading shared libraries: libntopreport-3.3.7.so: cannot open shared object file: No such file or directory".` I posted it on the ntop lists and was given the solution – just run `sudo ldconfig`

Installing from Repositories – Debian-based Distributions

Be sure that the computer is connected to the Internet, then just type sudo apt-get install ntop. The problem with this method is that you don't get the latest version of the application. For example the version of ntop in Ubuntu 8.04 repositories is version 3.3.2 while the latest stable version as of this writing is 3.3.7. The procedure is as follows:

1. Make sure that you have enabled the Universe repositories [uncomment the relevant line in /etc/apt/sources.lst]
2. Type sudo apt-get install ntop –y
3. Set the admin password by typing sudo ntop --set-admin-password
4. To start the application, type sudo ntop -u ntop –d
5. Ntop is setup to run at start-up by default.
6. You can stop, restart or stop it using sudo /etc/init.d/ntop start|stop|restart

Overview of Command line Parameters

To find out what command line options we can type ntop –h or ntop --help to get a listing of all possible parameters that ntop supports. Each parameter can be typed in either the short form – a single dash followed by a single alphabet [e.g. –i eth0] or the long form – double dashes followed by a string [e.g. interface eth0. In Linux, type man ntop to see all the possible parameters and their descriptions. Some examples of the ones a newbie will most likely use are as follows:

☑ Listen on the second Ethernet interface in a Linux machine:
- Short form: ntop –i eth1
- Long form: ntop --interface eth1

☑ Listen on all two Ethernet interfaces:
- Short form: ntop –i eth0,eth1
- Long form: ntop --interface eth0,eth1

☑ Listen on TCP port 5000 instead of the default 3000:
- Short form: ntop –w 5000
- Long form: ntop --http-server 5000

☑ Listen on TCP port 5005 when in secure [https] mode?:
- Short form: ntop –W 5005
- Long form: ntop --https-server 5005

☑ Treat all RFC1918 IP addresses as local and everything else as remote:
- Short form: ntop –m 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
- Long form: ntop --local-subnets 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16

☑ Don't resolve IP addresses into names:
- Short form: ntop –n
- Long form: ntop --numeric-ip-addresses

☑ Run ntop as a daemon in the background
- Short form: ntop –d
- Long form: ntop --daemon

☑ Only track statistics for local hosts:
- Short form: ntop –g
- Long form: ntop --track-local-hosts

Of course, we can combine multiple parameters on the same line like so:

ntop –i eth0,eth1 –w 5000 –W 5005 –d tells ntop to start and listen on Ethernet interfaces eth0 and eth1 [-i], listen on port 5000 [-w] for http and 5005 for secure http[-W] as well as make the ntop process run in the background as a daemon.

Default Parameters & Essential Ntop Configuration

In the Linux world, most applications have a configuration file named applicationname.conf in the /etc/ directory in which you tweak the application. In both of my investigations with ntop 3.3.2 installed through Ubuntu repositories and with ntop 3.3.7 compiled from source, no ntop.conf file is automatically created and none is given. However, I have come across sample ntop.conf files online. You can create your own ntop.conf file and place any command line parameters into the file and then launch ntop, pointing it to the file like so: `sudo ntop@/etc/ntop.conf`

The following list specifies the default parameters that ntop uses.

- ☑ Captures data from the eth0 network interface.
- ☑ Puts the network interface in promiscuous mode.
- ☑ Listens on TCP port 3000.
- ☑ Merges data from all physical interfaces.

By default, persistent ntop configuration is stored in the file called prefsCache.db in the user database directory

File Type	Location
Data files	/usr/local/share/ntop
Config files	/usr/local/etc/ntop
Run directory	/usr/local/var/ntop
Plugin files	/usr/local/lib/ntop/plugins
Database files	/usr/local/var/ntop

Login into Ntop's Web Interface

After installing ntop by any of the methods described above, setting the setting the admin password and then launching it, you can log into the web interface typing http://a.b.c.d:3000 where a.b.c.d is the IP address of the computer on which ntop is running (if you are trying to access if from the same computer, use http://127.0.0.1:3000). The default ports used to access ntop can be changed from both the preferences menu in the web UI or from command line that launches ntop.

NTOP MENU STRUCTURES

Menu Option	Description
Summary→Traffic	This page presents information in a set of tables and graphs under the following headings. Global Traffic Statistics: Traffic Report for Active Interface: Global Protocol Distribution: Global TCP/UDP Protocol Distribution: TCP/UDP Traffic Port Distribution: Last Minute View[6]:
Summary→Hosts	Gives host information for ALL hosts seen. The Traffic shown for each host can be by byte or packets. The bandwidth values are the percentage of the total bytes that ntop has seen on the interface, and the total of the values will NOT be 100% as local traffic will be counted TWICE (once as sent and again as received). Sent and Received bandwidth is shown in differently coloured bars.
Summary→Network Load	Shows graphs for network throughput for the past 10 minutes, 1 hour, 1day and 1 month. Click on the graph to display a table of the top 3 talkers every minute [by clicking on the Last 10 minute or Last Hour graphs] or hour [by clicking on the Last Day graph].
Summary→VLAN Info	Provides information about data sent and received by each VLAN in your network. The hosts that exist in each of the VLANs are also listed.
Summary→Network Flows	This lists information about any specific, user-defined flow rules.
All Protocols→Traffic	Displays a table that lists for each host seen, how much data the host has transferred, what percentage of total traffic since ntop has been running it represents, and amount of traffic sent by some key protocols [TCP,UDP,ICMP,ICMPv6,DLC,IPC,RARP,Appletalk,GRE,IPv6,OSPF,IPSec and Other protocols]
All Protocols→Throughput	Displays a table for network throughput. You can choose to see this information for Local hosts only or Remote hosts only or all hosts and for each option, you can view either data sent, data received or total data sent and received. By default, throughput is shown for all VLANs but you can choose to limit the information to a specific VLAN. As an example, when I want to view the highest consumers of Internet bandwidth, I select Local hosts only, data received and for all VLANs
All Protocols→Activity	Displays a table that shows hourly traffic per host. The percentage value for a given host is the traffic for that host during that hour divided by the total traffic for that host for the last 24 hours. The cell [host, hour] has one of 4 possible colours depending on percentage of traffic sent in that hour.

[6] Sum (total traffic per port) = 2 x (total IP traffic) because the traffic per port is counted twice (sent and received). This report includes broadcast packets.

Menu Option	Description
	For 0%, the cell is coloured white, for 0% - 25%, it is coloured pale cyan, for 25% - 75 % it is coloured pale green and for 75% - 100% it is coloured red. In practice I find this useful in validating claims by users that they have not been online for some specific period – ntop can give me data to say they are either not telling the truth or that their systems has been compromised by malware which is initiating all that network activity.
IP→Summary→Traffic	Displays a table that lists for each IP host seen, how much data the host has transferred, what percentage of total traffic since ntop has been running it represents, and amount of traffic sent by some key TCP/IP protocols [FTP, HTTP, DNS, Telnet, NBios-IP, Mail, DHCP-BOOTP, SNMP, NNTP, NFS/AFS, VoIP, X11, SSH, Gnutella, Kazaa, WinMX, DC++, eDonkey, BitTorrent, Messenger, Other IP]. You can display this information for Local, Remote or All hosts and for data sent, received or sent and received as well as per VLAN or all VLANs.
IP→Summary→Multicast	Displays a table of all multicast groups and sources and how much data each source has sent or how much data each group has received.
IP→Summary→Internet Domain	Displays traffic statistics for all Internet [think DNS] domains. For TCP/IP, sent/received data in kilobytes and as a percentage for TCP, UDP and for both are shown. For ICMP, sent/received traffic for IPv4 and IPv6 are shown.
IP→Summary→Networks	
IP→Summary→ASs	Displays a list of the BGP Autonomous Systems that your traffic traverses.
IP→Summary→Host Clusters	Displays traffic information aggregated by pre-defined host clusters. You can click on each cluster to drill down to traffic statistics for hosts within that cluster.
IP→Summary→Distribution	Displays a pie chart that shows the relative amount of traffic locally, Local to Remote and Remote to Local. For each of those traffic categories, a table provides more details broken down by IP protocol.
IP→Traffic Directions→Local to Local	Displays for each local host [DNS or NetBIOS name]: the IP address as well as data sent and received both in kilobytes and as a percentage. Small icons attached to the hosts column give good indicators of services [http, mail, p2p etc] as well as health status flags. At the bottom of the page is a small table that summarizes total traffic, total data sent and received as well as the used bandwidth for the period that ntop has been up.
IP→Traffic Directions→Local to Remote	Provides same information as above but limited statistics for traffic that originate from local hosts destined for remote hosts.
IP→Traffic Directions→Remote to Local	Provide per host traffic statistics for traffic that originates from remote hosts destined for local hosts.
IP→Traffic Directions→Remote to Remote	Provide per host traffic statistics for traffic that originates from remote hosts destined for other remote

Menu Option	Description
	hosts. Depending upon your setup, this page might not have any data e.g. when using ntop to monitor outbound traffic from my network, traffic from remote hosts that never come into my network will obviously remain unknown to ntop.
IP→Local→Routers	
IP→Local→Ports Used	Displays a table that lists for each service [e.g. ftp, telnet, and http] as identified by TCP/UDP port, the IP addresses of clients and servers using that service.
IP→Local→Host Fingerprint	Displays the Operating Systems of hosts that have been detected on the network. The accuracy of this feature depends on the OS fingerprint databases that are used by ettercap.
IP→Local→Host Characterization	Displays a table that identifies what type of device a host is[L2 switch, gateway, printer] and what kind of services run on it [VoiP, NTP/DNS server, Mai, Directory, HTTP, FTP, DHCP, WINS services, whether the host is running any peer-to-peer programs and whether the host is healthy or not]
IP→Local→Network Traffic Map	Draws a network traffic map that shows graphically which hosts are accessing which other ones.
IP→Local→Local Host Matrix	Displays a matrix of hosts on your local subnet and how much traffic they exchange with each other.
Utils→Data Dump	Provides a page where you can dump ntop statistics about known hosts, local traffic matrix, per interface information or information about configured network flows into various file formats [text, xml, perl, python, php and json]
Utils→View Log	This page displays the last 50 ntop log messages of priority INFO or higher.
Plugins→cPacket	This plugin is used collect traffic statistics emitted by cPacket's cTap devices. Received flow data is reported as a separate 'NIC' in the regular ntop reports – just like NetFlow virtual interfaces. Remember to switch the reporting NIC.
Plugins→Last Host Seen	This plugin produces a report about the last time packets were seen from each specific host. A note card database is available for recording additional information.
Plugins→ICMP Watch	This plugin produces a report about the ICMP packets that ntop has seen. The report includes each host, byte and per-type counts (sent/received).
Plugins→NetFlow	Offers options for viewing and configuring ntop as a NetFlow collector
Plugins→PDA	Options for viewing and configuring access to ntop from PDAs using WAP.
Plugins→Remote	This plugin allows remote applications to access ntop data
Plugins→Round Robin Databases	Offers options for viewing and configuring round robin databases – the only way that ntop keeps data that survives sessions.
Plugins→sFlow	Offers options for viewing and configuring ntop as an sFlow collector and analyzer.
Plugins→All	Displays in tabular form, a single page where you can view the status of , activate and configure various plugins. You will also find version information for each plugin as well as its author.

Menu Option	Description
Admin→Switch NIC	Allows you switch between various sources of data for ntop. All the network cards as well as NetFlow interfaces [if any have been configured in the NetFlow plugin] are listed for you to select one.
Admin→Configure→Startup	This brings up a page where you can configure start-up options for ntop. Most of the ntop options that you can specify on the command line have parallels here.
Admin→Configure→Preferences	Brings a page where you can set preferences for ntop. Most of the command line parameters have equivalents on this page. Typically, you assign a value of 0 to turn off an option or 1 to turn it on.
Admin→Configure→Packet Filter	Allows you set a filter expression that determines what kind of traffic ntop analyzes.
Admin→Configure→Reset Stats	Flush all host information ntop has in memory and start counting afresh.
Admin→Configure→Web Users	Configure a list of usernames and passwords for people who can use ntop
Admin→Configure→Protect URLs	Configure access to various pages of ntop and which users have access to them
Admin→Shutdown	Shut down the ntop programme.

Sample Screenshots of Ntop in Action

Summary→Traffic

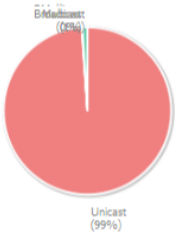
Global Traffic Statistics

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth1	eth1	Ethernet		0	1518	14	0.0.0.0	::/0
Local Domain Name	abu.edu.ng								
Sampling Since	Fri Sep 5 13:37:17 2008 [40:29]								
Active End Nodes	23633								

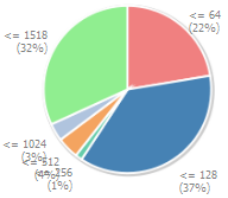
Traffic Report for 'eth1' [switch]

Packets

Dropped (libpcap)	4.6%	92,807
Dropped (ntop)	0.0%	0
Total Received (ntop)		2,012,371
Total Packets Processed		1,563,697
Unicast	98.9%	1,546,880
Broadcast	0.1%	867
Multicast	1.0%	15,950



Shortest		60 bytes
Average Size		623 bytes
Longest		1,518 bytes
Size <= 64 bytes	28.7%	495,449
64 < Size <= 128 bytes	47.6%	821,602
128 < Size <= 256 bytes	1.7%	28,869
256 < Size <= 512 bytes	5.4%	92,969
512 < Size <= 1024 bytes	4.4%	75,248
1024 < Size <= 1518 bytes	41.0%	707,159
Size > 1518 bytes	0.0%	0

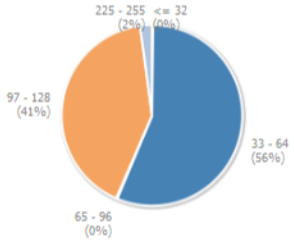


Packets too long [> 1518]	34.7%	598,865
Bad Packets (Checksum)	0.0%	4

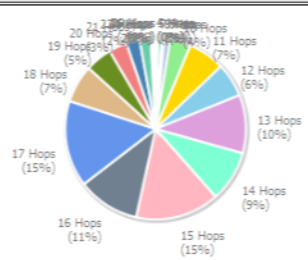
Traffic

Total		1.2 GBytes [1,818,361 Pkts]
IPv4 Traffic		1.2 GBytes [1,818,175 Pkts]
Fragmented IPv4 Traffic		0 [0.0%]
Non IPv4 Traffic		2.5 MBytes

Average TTL		78
TTL <= 32	0.2%	2,877
32 < TTL <= 64	56.1%	1,020,225
64 < TTL <= 96	0.2%	3,267
96 < TTL <= 128	41.4%	752,903
128 < TTL <= 160	0.0%	2
160 < TTL <= 192	0.0%	107
192 < TTL <= 224	0.0%	0
224 < TTL <= 256	2.0%	37,253



Remote Hosts Distance



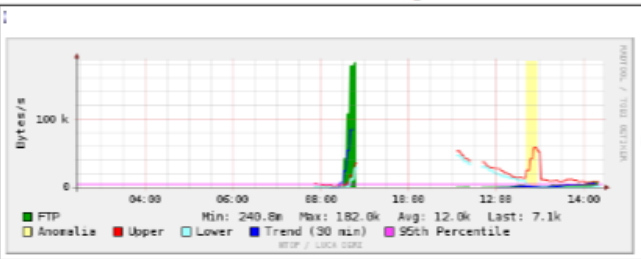
Network Load

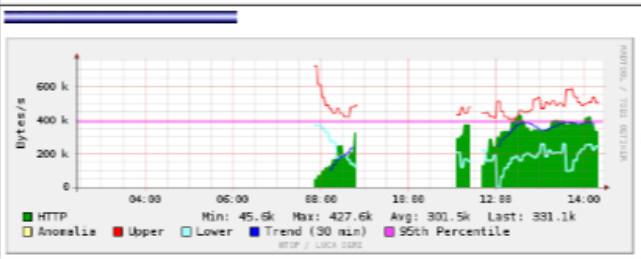
Actual	3.6 Mbit/s	601.4 Pkt/s
Last Minute	3.0 Mbit/s	557.2 Pkt/s
Last 5 Minutes	3.0 Mbit/s	560.6 Pkt/s
Peak	4.3 Mbit/s	819.4 Pkt/s
Average	3.4 Mbit/s	631.2 Pkt/s

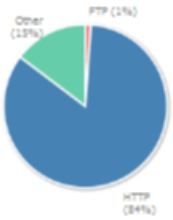
Historical Data [ ]

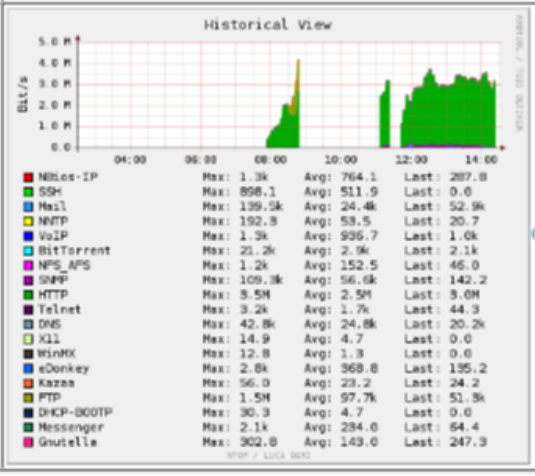
Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Flows	Accumulated Percentage / Historical Protocol View
FTP	15.3 MBytes	1,389	1.3%
HTTP	1.0 GBytes	30,171	85.8%
Other TCP/UDP-based Protocols	122.9 MBytes	459,303	10.1%
Accumulated View			
Historical View			









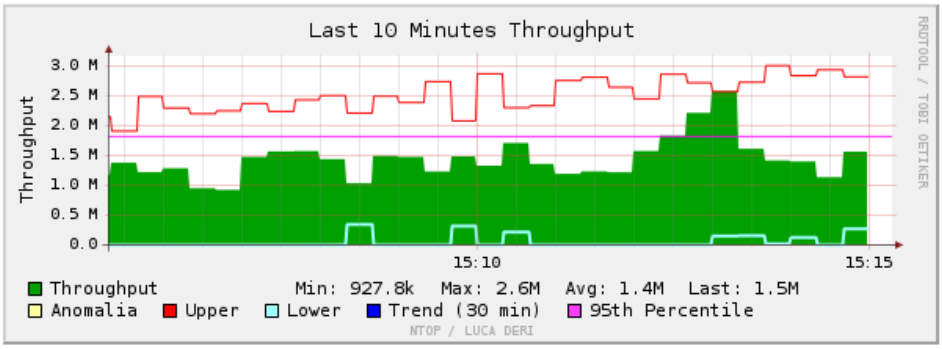
SUMMARY→HOSTS

Host Information

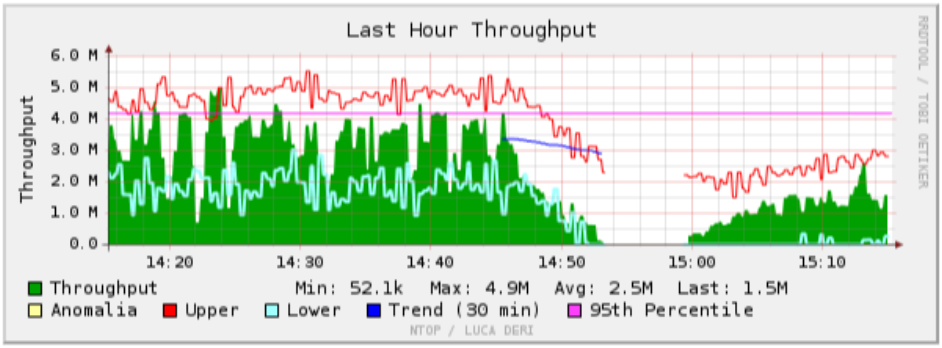
Traffic Unit: Bytes
VLAN: All
Subnet: All

Host	Domain	IP Address	MAC Address	Community	Other Name(s)	Bandwidth	Nw Board Vendor	Hops Distance	Host Contacts	Age/Inactivity		AS
76.9.18.107 (vlan 1)		76.9.18.107						7	20	14:21	0 sec	
10.5.5.2 (vlan 1)		10.5.5.2	00:17:08:54:AF:CF						12	14:59	5 sec	
10.5.5.19 (vlan 1)		10.5.5.19	00:17:08:54:AF:CF						714	14:13	0 sec	
10.0.0.138 (vlan 1)		10.0.0.138	00:0C:42:0F:37:1D						1622	15:01	0 sec	
10.0.0.14 (vlan 1)		10.0.0.14	00:14:C2:D5:76:97						475	11:24	0 sec	
192.168.5.18 (vlan 1)		192.168.5.18	00:17:08:54:AF:CF						194	14:52	2 sec	
192.168.4.80 (vlan 1)		192.168.4.80	00:17:08:54:AF:CF						52	9:52	0 sec	
10.0.0.7 (vlan 1)		10.0.0.7	00:16:D4:97:5A:D9						412	11:16	0 sec	
192.168.8.74 (vlan 1)		192.168.8.74	00:17:08:54:AF:CF						102	11:31	2 sec	
l1.ycs.vip.a2s.yahoo.com (vlan 1)		209.73.188.78						10	30	13:58	0 sec	
199.93.43.126 (vlan 1)		199.93.43.126						7	10	4:14	7:36	
128.107.229.50 (vlan 1)		128.107.229.50						13	6	15:00	0 sec	
146.82.206.219 (vlan 1)		146.82.206.219						11	2	1:48	0 sec	
10.10.100.15 (vlan 1)		10.10.100.15	00:17:08:54:AF:CF						132	14:08	10 sec	
192.168.4.13 (vlan 1)		192.168.4.13	00:17:08:54:AF:CF						145	11:49	0 sec	
192.168.4.15 (vlan 1)		192.168.4.15	00:17:08:54:AF:CF						196	9:35	0 sec	
192.168.4.39 (vlan 1)		192.168.4.39	00:17:08:54:AF:CF						80	14:50	0 sec	
192.168.8.70 (vlan 1)		192.168.8.70	00:17:08:54:AF:CF						34	12:58	2:06	
192.168.8.16 (vlan 1)		192.168.8.16	00:17:08:54:AF:CF						2304	10:28	0 sec	
192.168.8.23 (vlan 1)		192.168.8.23	00:17:08:54:AF:CF						174	15:04	0 sec	
217.132.176.1 (vlan 1)		217.132.176.1							1	8 sec	8:07	
85.201.40.153 (vlan 1)		85.201.40.153						15	2	8:02	4:22	
c-24-60-179-84.hsd1.ma.comcast.net (vlan 1)		24.60.179.84							1	0 sec	9:30	
s010600e0b881cd86.wp.shawcable.net (vlan 1)		24.78.179.164							1	6 sec	4:04	
192.168.2.4 (vlan 1)		192.168.2.4	00:E0:4C:03:49:F2						1	3 sec	9:36	
a96-7-67-91.deploy.akamaitechnologies.com (vlan 1)		96.7.67.91						7	2	1:02	0 sec	
87.110.45.177 (vlan 1)		87.110.45.177						15	2	0 sec	4:22	
w2k3-web28.prod.netsolhost.com (vlan 1)		205.178.152.28						17	2	28 sec	1:30	
72.231.18.102 (vlan 1)		72.231.18.102							1	2 sec	6:36	
213.114.41.86 (vlan 1)		213.114.41.86							1	0 sec	3:57	
93.94.185.69 (vlan 1)		93.94.185.69							1	48 sec	9:07	
118.166.233.114 (vlan 1)		118.166.233.114						21	2	1 sec	4:33	
host86-146-41-124.range86-146.btcentralplus.com (vlan 1)		86.146.41.124						20	2	0 sec	8:52	
host85-26-dynamic.24-79-r.retail.telecomitalia.it (vlan 1)		79.24.26.85							1	6 sec	6:54	
69.116.14.158 (vlan 1)		69.116.14.158							1	0 sec	2:54	
65.191.135.7 (vlan 1)		65.191.135.7							1	2 sec	8:30	

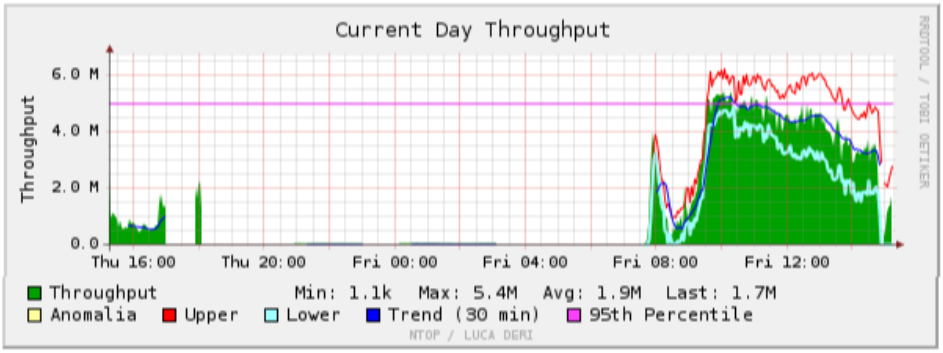
Network Load Statistics



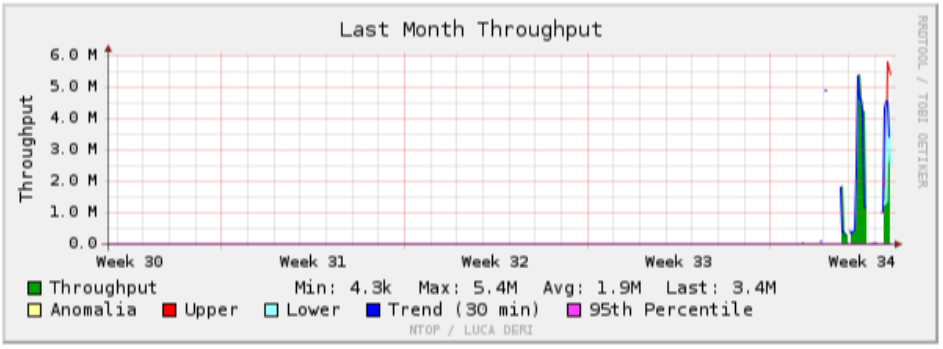
Time [Fri Aug 22 15:05:18 2008 through now]



Time [Fri Aug 22 14:15:18 2008 through now]



Time [Thu Aug 21 15:15:18 2008 through now]



Time [Wed Jul 23 15:15:18 2008 through now]

IP→SUMMARY→MULTICASTS

Multicast Statistics

Host	Domain	Pkts Sent	Data Sent	Pkts Rcvd	Data Rcvd
ospf-all.mcast.net (vlan 1)		0	0	1,519	152.5 KBytes
10.0.0.1 (vlan 1)		269	27.2 KBytes	0	0
10.0.0.2 (vlan 1)		278	27.9 KBytes	0	0
10.0.0.3 (vlan 1)		277	27.9 KBytes	0	0
10.0.0.4 (vlan 1)		278	27.8 KBytes	0	0
10.0.0.7 (vlan 1)		66	10.2 KBytes	0	0
10.0.0.14 (vlan 1)		6	966	0	0
10.0.0.18 (vlan 1)		1	78	0	0
10.0.0.23 (vlan 1)		1	143	0	0
10.0.0.29 (vlan 1)		282	29.0 KBytes	0	0
10.0.0.30 (vlan 1)		270	27.1 KBytes	0	0

CONFIGURING PERSISTENT STORAGE USING RRDS

As mentioned earlier, the only historical data that ntop stores is actually in Round Robin Databases, used in producing all those cute traffic graphs you see for various statistics and for storing information over long periods of time such that the size of the database doesn't grow out of control.

To weak RRD in ntop, click **Plugins→Round Robin Databases→Configure** to bring up the RRD configuration page. Some of the configurable parameters are described in the following table:

Parameter	Description
Dump Interval	Specifies how often [in seconds] traffic data that is in memory is stored permanently.
Dump Hours	Specifies how many hours worth of 'Interval' data is stored permanently
Dump Days	Specifies how many days of hourly data are stored.
Dump Months	Specifies how many months of daily data are stored.
Data to Dump	Specifies what data to dump into the round robin databases. You can dump data about flows, hosts, interfaces or the traffic matrix
RRD Detail	For each or all of the Data items listed you selected, how much detail do you want to dump. The next table gives the specifics about various levels of detail.

The table lists the differences between different host level details. The counts for each level are in addition for the counts for all lower levels.

Level	Counts
Low	pktSent/pktRcvd and bytesSent/bytesRcvd
Medium	pktDuplicatedAckSent/pktDuplicatedAckRcvd, pktBroadcastSent, bytesBroadcastSent, pktMulticastSent, bytesMulticastSent, pktMulticastRcvd, bytesMulticastRcvd, bytesSentLoc, bytesSentRem, bytesRcvdLoc, bytesRcvdFromRem,

	ipBytesSent, ipBytesRcvd, tcpSentLoc, tcpSentRem, tcpRcvdLoc, tcpRcvdFromRem, tcpFragmentsSent, tcpFragmentsRcvd, udpSentLoc, udpSentRem, udpRcvdLoc, udpRcvdFromRem, udpFragmentsSent, udpFragmentsRcvd, icmpSent, icmpRcvd, icmpFragmentsSent, icmpFragmentsRcvd, ipv6Sent, ipv6Rcvd Non-IP Counts: stpSent, stpRcvd, ipxSent, ipxRcvd, osiSent, osiRcvd, dlcSent, dlcRcvd, arp_rarpSent, arp_rarpRcvd, arpReqPktsSent, arpReplyPktsSent, arpReplyPktsRcvd, decnetSent, decnetRcvd, appletalkSent, appletalkRcvd, netbiosSent, netbiosRcvd, otherSent, otherRcvd per-protocol Sent/Rcvd
High	totContactedSentPeers, totContactedRcvdPeers per-IP-protocol Sent/Rcvd, e.g. IP_HTTP.

For a detailed look at how RRDs are used in ntop, see Burton M. Strauss' paper which is downloadable from sourceforge.net.

Using ntop as a NetFlow Collector

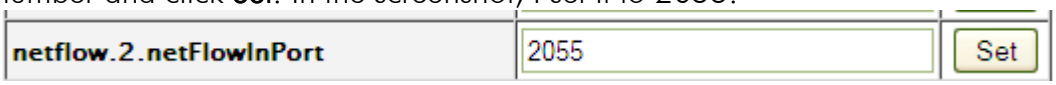
To achieve this, you first need to do three things:

1. Prepare [configure] ntop to receive NetFlow information from a NetFlow probe.
2. Configure the NetFlow probe to send its flow information to ntop.
3. Switch to the virtual NetFlow interface so that ntop analyzes traffic from NetFlow rather than from its local interfaces.

The procedures for each step are detailed below.

Configure Ntop NetFlow Plugin to Receive NetFlow Data

1. Click **Plugins→NetFlow→Activate** to activate the NetFlow plugin.
2. Click **Plugins→NetFlow→View/Configure** to see current NetFlow virtual interfaces and possible add more.
3. To set the port on which ntop listens for NetFlow information, go to **Admin→Preferences**, look for the parameter called "netflow.2.netFlowInPort" and type in the desired port number and click **Set**. In the screenshot, I set it to 2055.



Configure the NetFlow Probe to export Data to Ntop

The procedure on Cisco routers assuming your router's IOS version is 12.2(T) or later, is as follows:

1. Configure the interface to capture flows into the NetFlow cache.

```
Router(config)# ip cef
Router(config)# interface ethernet 1/0 .
Router(config-if)# ip flow ingress
```

2. Configure the router to export the NetFlow data to ntop

```
Router(config)# ip flow-export version 9
Router(config)# ip flow-export destination a.b.c.d 2055
```

a.b.c.d is the IP address of your ntop server which has been configured to listen for NetFlow data on port 2055.

If you happen to be using a Mikrotik RouterOS-based device, the procedure is as follows:

1. Enable traffic flow on the route:

```
[admin@MikroTik] ip traffic-flow> set enabled=yes
```

2. Specify the IP address of your ntop server and port on which it is listening for NetFlow data.

```
[admin@MikroTik] ip traffic-flow target> add address=192.168.0.2:2055 version=9
```

Configure Ntop to Analyze the NetFlow Data

This just means switching the Interface from which ntop gets its data from. On the **Summary→Traffic** page, in the table titled **Global Traffic** Statistics, the row titled **Network Interface(s)** lists the available interfaces from which ntop is getting data. If you properly configured the NetFlow plugin, a NetFlow interface should be listed here [**NetFlow.interfaceX**] The next table with heading **Traffic Report for 'eth0' [switch]** tells you that ntop is currently analyzing data that comes in through interface eth0. The switch link when clicked on takes you to a dialog box [also accessed by clicking **Admin→Switch NICs**] that lists the various interfaces available on the system [both physical and virtual interfaces like NetFlow interfaces] and lets you choose which one you want ntop to report traffic for. Simply select the NetFlow interface.

Ntop Usage Scenarios

Who Are The Top Internet Bandwidth Users on my Network?

The way most web browsing works, most of the traffic is usually inbound from the Internet [text, pictures, sound, video], in response to very little that is going out [like HTTP Get requests and other commands]. Consider a user downloading huge files [pirated movies, pictures, porn, iso images?], he might send in a small request during a 20 minute interval that results in the transfer of 650MB of data inbound to him. Thus, the critical bandwidth you are interested in here is the bandwidth that each host on your local network receives. To see the top bandwidth consumers, proceed as follows:

1. Select **All Protocols→Traffic** menu option.
2. In the **Hosts** dropdown listbox, select **Local Only**
3. In the **Data** dropdown listbox, select **Received Only**
4. Click on the VLAN you are interested in or **ALL** to see traffic for all VLANs.
5. Click on the Data column name to sort by data and percentage.

Flipping this concept on its back, if a host on your network is sending more traffic than it is receiving, then that host is offering 'server' services of some kind e.g. a web server, a P2P host that is sharing data and others are downloading from it, an FTP server etc.

Another page that can give valuable information specific to the IP protocol [recall that ntop supports IPX, AppleTalk and other protocols] is the **IP→Traffic Directions→Local to Remote** menu option which tabulates for each local host, the amount of traffic sent and or received from remote locations. Always make sure to sort on the Data column.

Host ⇩	IP Address	Data Sent		Data Rcvd	
bigbrother (vlan 1)	10.0.0.25	228.9 KBytes	0.6 %	221.6 KBytes	0.0 %
10.0.0.1 (vlan 1)	10.0.0.1	88.6 KBytes	0.2 %	0	0.0 %
10.0.0.2 (vlan 1)	10.0.0.2	114.1 KBytes	0.3 %	0	0.0 %
10.0.0.3 (vlan 1)	10.0.0.3	97.1 KBytes	0.2 %	0	0.0 %
10.0.0.4 (vlan 1)	10.0.0.4	89.9 KBytes	0.2 %	0	0.0 %
10.0.0.7 (vlan 1)	10.0.0.7	21.9 MBytes	55.0 %	1.3 GBytes	68.5 %
10.0.0.13 (vlan 1)	10.0.0.13	6.5 MBytes	16.2 %	468.8 MBytes	24.0 %
10.0.0.18 (vlan 1)	10.0.0.18	1.2 MBytes	3.1 %	48.8 MBytes	2.5 %
10.0.0.19 (vlan 1)	10.0.0.19	267.2 KBytes	0.7 %	19.2 MBytes	1.0 %
10.0.0.29 (vlan 1)	10.0.0.29	96.1 KBytes	0.2 %	0	0.0 %
10.0.0.30 (vlan 1)	10.0.0.30	88.6 KBytes	0.2 %	0	0.0 %
10.0.0.193 (vlan 1)	10.0.0.193	163	0.0 %	261	0.0 %
10.0.0.194 (vlan 1)	10.0.0.194	956.4 KBytes	2.3 %	6.2 MBytes	0.3 %
10.10.100.13 (vlan 1)	10.10.100.13	613.1 KBytes	1.5 %	5.8 MBytes	0.3 %
10.10.100.14 (vlan 1)	10.10.100.14	516.2 KBytes	1.3 %	5.8 MBytes	0.3 %
10.10.100.20 (vlan 1)	10.10.100.20	1.9 MBytes	4.7 %	11.1 MBytes	0.6 %
10.10.100.22 (vlan 1)	10.10.100.22	109.2 KBytes	0.3 %	1.2 MBytes	0.1 %

What Websites do the Top Bandwidth Wasters Visit?

You might need this information to ascertain whether whatever it is those top bandwidth users are doing is something that benefits your organization? After finding out who the top bandwidth users are as described above, each of the hosts listed is a link to detailed host information. Just click on the host you are interested in, scroll down to the bottom of the page to the table called **Last Contacted Peers**. This table gives a list of all other hosts that the host of interest has been in contact with.

Last Contacted Peers

Sent To	IP Address	Received From	IP Address
91.187.115.253 (vlan 1)	91.187.115.253	sb.google.com (vlan 1)	66.249.89.91
www.fig.net (vlan 1)	131.165.67.2	cds219.lon.llnw.net (vlan 1)	87.248.211.149
amontpellier-157-1-162-57.w90-14.abo.wanadoo.fr (vlan 1)	90.14.185.57	118.100.213.243 (vlan 1) [IP]	118.100.213.243
74.13.153.226 (vlan 1)	74.13.153.226	69.253.109.3 (vlan 1)	69.253.109.3
69.253.109.3 (vlan 1)	69.253.109.3	cellbioed.highwire.org (vlan 1)	171.66.124.194
cellbioed.highwire.org (vlan 1)	171.66.124.194	hs.imesh.com (vlan 1)	192.114.71.235
sb.google.com (vlan 1)	66.249.89.91	au.download.windowsupdate.com (vlan 1)	204.160.107.126
cds219.lon.llnw.net (vlan 1)	87.248.211.149	guru.grisoft.com (vlan 1)	193.86.3.36
Total Contacts	18621	Total Contacts	16507

Another table just below the one above identifies what applications the host in question is using.

TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
telnet	23	42/7.2 KBytes	76.13.15.40 (vlan 1)		
domain	53	1138/107.2 KBytes	10.0.0.1 (vlan 1) [IP]		
www	80	26468/29.6 MBytes	sb.google.com (vlan 1)		
ntp	123	2/96	clock.via.net (vlan 1)		
netbios-ns	137	3/150	bpcrfectchoice1.com (vlan 1)		
snmp	161	8/616	172.24.194.57 (vlan 1)		
https	443	1207/785.8 KBytes	voipa.sip.yahoo.com (vlan 1)		

What Websites Get the Most Traffic from within my Organization?

Again following the logic above, the most popular websites are those that receive the highest amounts of data from your local users. Note that a remote host may have sent higher amounts of data into your network but all may be due to requests from a single host [e.g. requesting for streaming audio/video]. As an example, suppose that everyone on getting into the office logs gets to Google to check their email, then the IP address/addresses that host Gmail will receive many requests. Proceed as follows to produce a listing of such websites:

1. Select **All Protocols→Traffic** menu option.
2. In the **Hosts** dropdown listbox, select **Remote Only**
3. In the **Data** dropdown listbox, select **Received Only**
4. Click on the VLAN you are interested in or **ALL** to see traffic for all VLANs.
5. Click on the Data column name to sort by data and percentage.

Network Traffic [All Protocols]: Remote Hosts - Data Received

Hosts: Remote Only

VLAN: [1] [3] [All]

Data: Received Only

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)
apache2-dap.atomic.dreamhost.com (vlan 1)		1.6 MBytes	19.2 %	1.6 MBytes	0	0	0	0	0	0	
acm.org.s7a1.psmtp.com (vlan 1)		495.0 KBytes	5.9 %	493.9 KBytes	0	0	0	0	0	0	
87.248.211.215 (vlan 1) [IP]		253.2 KBytes	3.0 %	252.5 KBytes	0	686	0	0	0	0	
webmail.excite.com (vlan 1)		167.2 KBytes	2.0 %	167.0 KBytes	0	0	0	0	0	0	
ad.yieldmanager.com (vlan 1)		147.6 KBytes	1.8 %	147.3 KBytes	0	0	0	0	0	0	
us.bc.yahoo.com (vlan 1)		95.4 KBytes	1.1 %	95.3 KBytes	0	0	0	0	0	0	
update.microsoft.com (vlan 1)		79.7 KBytes	1.0 %	79.5 KBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		78.8 KBytes	0.9 %	78.8 KBytes	0	0	0	0	0	0	
cfcluster.srv.ualberta.ca (vlan 1)		77.0 KBytes	0.9 %	77.0 KBytes	0	0	0	0	0	0	
msnbcmedia3.msn.com (vlan 1)		75.8 KBytes	0.9 %	75.8 KBytes	0	0	0	0	0	0	
thumbnails.truveo.com (vlan 1)		70.9 KBytes	0.8 %	70.9 KBytes	0	0	0	0	0	0	
rs9113.rapidshare.com (vlan 1)		69.3 KBytes	0.8 %	69.3 KBytes	0	0	0	0	0	0	
acm.org.s7a2.psmtp.com (vlan 1)		67.5 KBytes	0.8 %	67.4 KBytes	0	0	0	0	0	0	

Which Websites' Traffic Consumes Most of my Bandwidth?

You might need this information in order to implement proactive caching on your proxy server or to block popular bandwidth-wasting destinations like download sites. What we are interested in here is how much data the remote host sent [to our network]

1. Select **All Protocols→Traffic** menu option.
2. In the **Hosts** dropdown listbox, select **Remote Only**
3. In the **Data** dropdown listbox, select **Sent Only**
4. Click on the VLAN you are interested in or **ALL** to see traffic for all VLANs.
5. Click on the Data column name to sort by data and percentage.

Network Traffic [All Protocols]: Remote Hosts - Data Sent

Hosts: Remote Only

VLAN: [1] [3] [All]

Data: Sent Only

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)AR
87.248.211.215 (vlan 1) [IP]		6.6 MBytes	6.6 %	6.6 MBytes	0	0	0	0	0	0	
rs9113.rapidshare.com (vlan 1)		3.8 MBytes	3.8 %	3.8 MBytes	0	0	0	0	0	0	
rs103gc.rapidshare.com (vlan 1)		3.3 MBytes	3.3 %	3.3 MBytes	0	0	0	0	0	0	
au.download.windowsupdate.com (vlan 1)		3.2 MBytes	3.2 %	3.2 MBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
fpdownload2.macromedia.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
searchportal.information.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
rs330l33.rapidshare.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
us.js2.yimg.com (vlan 1)		1.8 MBytes	1.8 %	1.8 MBytes	0	0	0	0	0	0	
85.112.115.50 (vlan 1) [IP]		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
akamai.avg.com (vlan 1)		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
d.yimg.com (vlan 1)		1.6 MBytes	1.6 %	1.6 MBytes	0	0	0	0	0	0	

Remote traffic data can also be obtained specifically for the IP protocol by choosing **IP→Traffic Directions→Remote to Local** and then sorting by **Data Sent** or **Data Received**. A sample screenshot is shown [and tells me that three sites with IP addresses 68.178.228.187, 76.9.18.120 and 85.17.230.66 are responsible for consuming more than 50% of my download bandwidth!!!].

Remote to Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
ip-68-178-228-187.ip.secureserver.net (vlan 1)	68.178.228.187	78.3 MBytes	28.1 %	613.4 KBytes	5.0 %
76.9.18.120 (vlan 1)	76.9.18.120	48.8 MBytes	17.5 %	253.4 KBytes	2.1 %
w17.easy-share.com (vlan 1)	85.17.230.66	40.3 MBytes	14.4 %	196.1 KBytes	1.6 %
80.239.137.33 (vlan 1)	80.239.137.33	24.7 MBytes	8.9 %	309.4 KBytes	2.5 %
208.48.186.86 (vlan 1)	208.48.186.86	17.8 MBytes	6.4 %	145.8 KBytes	1.2 %
80.70.172.78 (vlan 1)	80.70.172.78	9.3 MBytes	3.3 %	6.1 KBytes	0.1 %
assessment-prod-nv.cisco.com (vlan 1)	128.107.229.51	8.4 MBytes	3.0 %	900.4 KBytes	7.3 %
38.96.182.20 (vlan 1)	38.96.182.20	6.0 MBytes	2.2 %	662.5 KBytes	5.4 %
cna-prod-nv.cisco.com (vlan 1)	128.107.229.50	5.4 MBytes	1.9 %	870.2 KBytes	7.1 %
64.215.158.132 (vlan 1)	64.215.158.132	4.8 MBytes	1.7 %	9.8 KBytes	0.1 %
66.90.103.49 (vlan 1)	66.90.103.49	4.0 MBytes	1.4 %	191.3 KBytes	1.6 %
205.128.73.126 (vlan 1)	205.128.73.126	2.8 MBytes	1.0 %	129.8 KBytes	1.1 %
67.199.128.41 (vlan 1)	67.199.128.41	2.2 MBytes	0.8 %	1.0 MBytes	8.5 %
xmlrpc.rhn.redhat.com (vlan 1)	209.132.177.100	1.6 MBytes	0.6 %	743.6 KBytes	6.1 %
cortona.webhosters.no (vlan 1)	63.247.138.183	1.5 MBytes	0.6 %	17.3 KBytes	0.1 %
66.48.78.209 (vlan 1)	66.48.78.209	1.4 MBytes	0.5 %	481.2 KBytes	3.9 %
67.199.128.42 (vlan 1)	67.199.128.42	1.3 MBytes	0.5 %	465.8 KBytes	3.8 %
l1.ycs.vip.a2s.yahoo.com (vlan 1)	209.73.188.78	1.3 MBytes	0.5 %	100.7 KBytes	0.8 %
87.104.113.106 (vlan 1)	87.104.113.106	1.0 MBytes	0.4 %	258.6 KBytes	2.1 %
76.9.18.128 (vlan 1)	76.9.18.128	1.0 MBytes	0.4 %	123.4 KBytes	1.0 %
unassigned-66.147.227.189.hrwebservices.net (vlan 1)	66.147.227.189	965.2 KBytes	0.3 %	84.2 KBytes	0.7 %
76.9.18.115 (vlan 1)	76.9.18.115	874.3 KBytes	0.3 %	124.1 KBytes	1.0 %
ns1.globalconnex.net (vlan 1)	80.255.35.180	788.5 KBytes	0.3 %	328.8 KBytes	2.7 %
f1.www.vip.re1.yahoo.com (vlan 1)	69.147.76.15	771.6 KBytes	0.3 %	96.8 KBytes	0.8 %
74.54.144.163 (vlan 1)	74.54.144.163	641.9 KBytes	0.2 %	76.1 KBytes	0.6 %
194.129.79.44 (vlan 1)	194.129.79.44	471.7 KBytes	0.2 %	169.5 KBytes	1.4 %
64.236.22.63 (vlan 1)	64.236.22.63	26.3 KBytes	0.0 %	12.4 KBytes	0.1 %
www4.cnn.com (vlan 1)	64.236.16.52	24.4 KBytes	0.0 %	5.8 KBytes	0.0 %
66.218.161.133 (vlan 1)	66.218.161.133	24.1 KBytes	0.0 %	7.8 KBytes	0.1 %
212.58.226.20 (vlan 1)	212.58.226.20	19.0 KBytes	0.0 %	918	0.0 %
cf-in-f19.google.com (vlan 1)	74.125.19.19	18.8 KBytes	0.0 %	9.9 KBytes	0.1 %
bs1b1.ads.vip.re2.yahoo.com (vlan 1)	68.142.228.136	17.1 KBytes	0.0 %	56.3 KBytes	0.5 %
ev1s-67-15-56-64.theplanet.com (vlan 1)	67.15.56.64	16.0 KBytes	0.0 %	30.1 KBytes	0.2 %
196.46.240.47 (vlan 1)	196.46.240.47	15.4 KBytes	0.0 %	3.0 KBytes	0.0 %
4.71.209.7 (vlan 1)	4.71.209.7	15.3 KBytes	0.0 %	33.9 KBytes	0.3 %
72.32.3.220 (vlan 1)	72.32.3.220	14.8 KBytes	0.0 %	5.5 KBytes	0.0 %
209.73.189.15 (vlan 1)	209.73.189.15	13.5 KBytes	0.0 %	724	0.0 %
fg-in-f190.google.com (vlan 1)	72.14.221.190	13.4 KBytes	0.0 %	777	0.0 %
58-65-236-153.myrdns.com (vlan 1)	58.65.236.153	13.2 KBytes	0.0 %	2.9 KBytes	0.0 %
89-145-77-122.as29017.net (vlan 1)	89.145.77.122	13.0 KBytes	0.0 %	10.0 KBytes	0.1 %
66.48.78.212 (vlan 1)	66.48.78.212	12.5 KBytes	0.0 %	1.4 KBytes	0.0 %
213.244.183.217 (vlan 1)	213.244.183.217	12.0 KBytes	0.0 %	19.4 KBytes	0.2 %
cf-in-f97.google.com (vlan 1)	74.125.19.97	11.9 KBytes	0.0 %	2.8 KBytes	0.0 %
a96-7-69-186.deploy.akamaitechnologies.com (vlan 1)	96.7.69.186	11.7 KBytes	0.0 %	3.8 KBytes	0.0 %
host2.itopsites.com (vlan 1)	72.52.152.216	11.6 KBytes	0.0 %	15.3 KBytes	0.1 %
vip1.cdn.cachefly.net (vlan 1)	205.234.175.175	11.4 KBytes	0.0 %	1.6 KBytes	0.0 %

[1 / 2]

Total Traffic	Data Sent	Data Rcvd	Used Bandwidth
290.8 MBytes	278.9 MBytes	12.0 MBytes	330.1 Kbit/s

What Applications are being used?

'Applications' in this context refers to network applications, and are essentially identified by the ports they use. DNS for example is an application whose server component always listens on UDP port 53. Although most peer-to-peer programmes by default use a specific range of ports, they can also use the ports of other well-known protocols like http [80] so ntop depends on header information to detect p2p programmes. The following ntop pages will give you this information:

- ☑ **Global TCP/UDP Protocol Distribution**, accessed from the **Summary→Traffic** page shows graphs of the most popular applications seen since ntop has was started.
- ☑ **Accumulated and Historical Views** at the bottom of the **Summary→Traffic** page also a nice graph of each application's [protocol] bandwidth utilization per time interval.
- ☑ **TCP/UDP: Local Protocol Usage** page accessed from the **IP→Local→Ports Used** menu option will list the applications being served and used by your local hosts. For each application, the IP addresses or names of local clients are listed as well as the local host that is serving the application.

Which Local Hosts Share the Most Data?

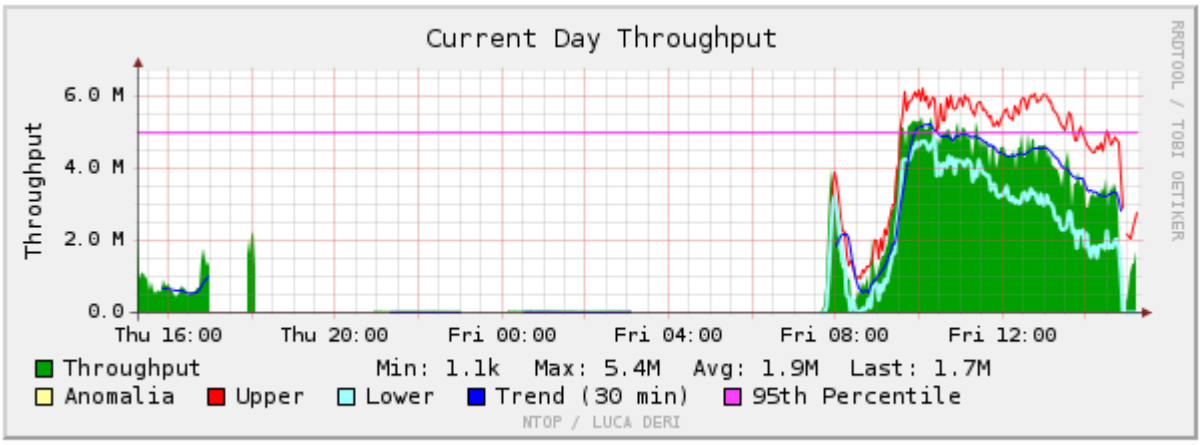
From my experience with ntop and from a logical understanding of the theory, this information is only possible for local hosts that are in the same broadcast domain as a physical interface of the ntop machine. Thus if you are using NetFlow probes in a subnet that is non-local to one of the interfaces of the ntop server, you won't get information about which pairs of local hosts are exchanging traffic. To see the local traffic matrix, click **IP→Local→Local Host Matrix.** A screenshot of such a page is shown below. I did notice that when configure ntop to only listen on one interface and that interface has no IP address and is plugged into a SPAN port, there won't be anything to display on this page.

IP Subnet Traffic Matrix

From \ To	10.0.0.1	10.0.0.2	10.0.0.3	10.0.0.7	10.0.0.10	10.0.0.13	10.0.0.17	10.0.0.18	10.0.0.19	10.0.0.22	10.0.0.25	ftp	nis-portal	10.0.0.29
10.0.0.1		220	219	4.1 KB	10.0 KB	130.4 KB	58.1 KB	124.9 KB	279.1 KB	1.0 MB	3.5 MB	90.9 KB	1.1 MB	3.4 MB
10.0.0.2	220													
10.0.0.3	219													
10.0.0.7	4.1 KB													
10.0.0.10	10.0 KB													
10.0.0.13	130.4 KB													
10.0.0.17	58.1 KB													
10.0.0.18	124.9 KB													
10.0.0.19	279.1 KB													
10.0.0.22	1.0 MB													
10.0.0.25	3.5 MB													
ftp	90.9 KB													
nis-portal	1.1 MB													
10.0.0.29	3.4 MB													

At what Time of the Day is the Network Most Utilized?

To answer this question, take a look at the **Summary→Network Load** page. Specifically the **Last Day** graph.



Time [Thu Aug 21 15:15:18 2008 through now]

In the sample screenshot above, I can deduce that on Friday, for some reason [network failure? router down? Power failure?] users only started trying to access the web around 7:45am and that peak traffic occurred at about 10 am. I can also deduce that there was some kind of interruption about 2pm. By looking at the **Current Month** graphs, you can establish a trend of traffic usage and so be able to detect anomalous behaviour.

Performing a Network Inventory

In case you want to find out what devices run which network services, which are the DHCP, DNS, Web servers? Which hosts are routers etc? The page to go is the **Local Hosts Characterization** page accessed from **IP→local→Hosts Characterization**. A screenshot is shown below:

Local Hosts Characterization

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/FTP/HTTP Server	DHCP/WINS Server	DHCP Client	P2P
192.168.4.80 (vlan 1)	X										
10.0.0.1 (vlan 1)	X					X					
10.0.0.7 (vlan 1)						X					
10.0.0.13 (vlan 1)						X					
10.0.0.18 (vlan 1)						X					
10.0.0.19 (vlan 1)	X					X					
bigbrother (vlan 1)	X					X					
egroupware (vlan 1)	X					X					
10.0.0.29 (vlan 1)	X					X					
10.0.0.193 (vlan 1)						X					
10.0.0.194 (vlan 1)	X					X					
10.10.100.20 (vlan 1)	X										
10.10.100.14 (vlan 1)	X										
Total	9 [40.9 %]				10						

Exporting Traffic Data

You might want to dump the current data that ntop has in its memory structures so that you can apply other analysis tools to it. To do this, click **Utils→Data Dump** to bring up the screen shown below. You can dump data about hosts, subnets, host matrix and per interface. Also you can dump the data in several formats that you can select from the dropdown list.

Report Type	Description	Action
Hosts	Dump information about known hosts	**Format:** text **Attributes List:** Long Dump Data
Hosts Matrix	Dump local hosts traffic matrix	**Format:** text **Attributes List:** Long Dump Data
Network Interfaces	Dump per-interface information	**Format:** text **Attributes List:** Long Dump Data
Network Flows	Dump traffic information of the configured network flows	**Format:** text **Attributes List:** Long Dump Data

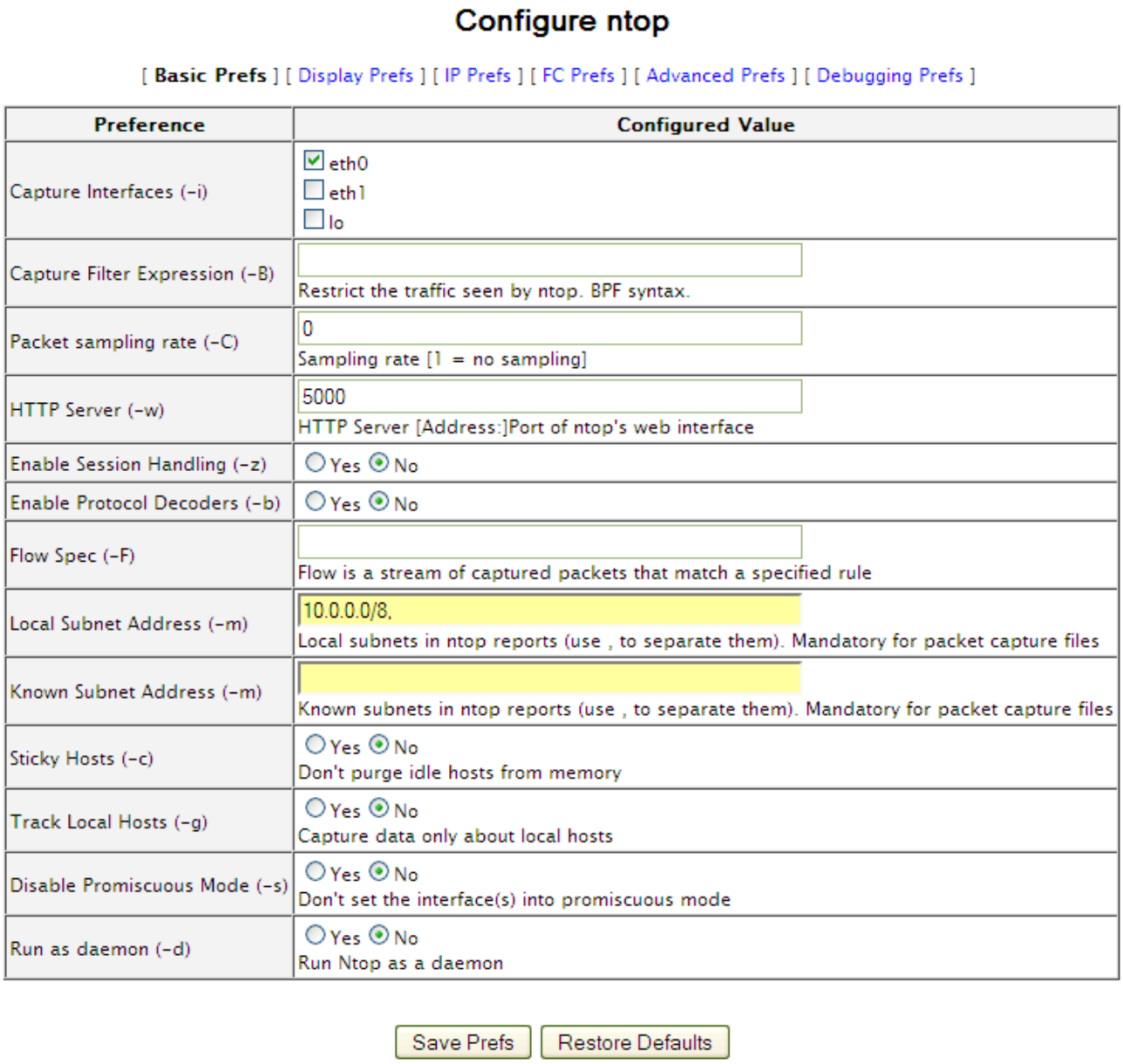
Detecting Network Security Violations?

In my opinion, the most obvious pointer to a security violation is when a host tries to contact too many other hosts, especially local hosts. This behaviour is allowable and expected for vulnerability scanners and network management servers. Outside of these two, a normal host that initiates contact with many other hosts could either be an intruder doing port scanning [nmap], ping sweep, a network virus or worm or even a peer-to-peer client. On the other hand, if a computer is acting as a server [either one the system admins deployed or a server service running on a user's computer – which is a network vulnerability], it will have many connections to it.

The first clue to a security violation that ntop gives you is with those little icons besides hosts in any listing of hosts [Summary→Hosts, All Protocols→Traffic, IP→Summary→Traffic etc]. A green flag represents low risk, yellow flag represents medium risk and red flag represent high risk. Other icons are shown if the host is a peer-to-peer server, VoIP client etc.

Configuring Startup Options

Just click **Admin→Configure→ Start-up Options** to display the following page.



Configure ntop

[**Basic Prefs**] [Display Prefs] [IP Prefs] [FC Prefs] [Advanced Prefs] [Debugging Prefs]

Preference	Configured Value
Capture Interfaces (-i)	☑ eth0 ☐ eth1 ☐ lo
Capture Filter Expression (-B)	Restrict the traffic seen by ntop. BPF syntax.
Packet sampling rate (-C)	0 Sampling rate [1 = no sampling]
HTTP Server (-w)	5000 HTTP Server [Address:]Port of ntop's web interface
Enable Session Handling (-z)	○ Yes ◉ No
Enable Protocol Decoders (-b)	○ Yes ◉ No
Flow Spec (-F)	Flow is a stream of captured packets that match a specified rule
Local Subnet Address (-m)	10.0.0.0/8, Local subnets in ntop reports (use , to separate them). Mandatory for packet capture files
Known Subnet Address (-m)	Known subnets in ntop reports (use , to separate them). Mandatory for packet capture files
Sticky Hosts (-c)	○ Yes ◉ No Don't purge idle hosts from memory
Track Local Hosts (-g)	○ Yes ◉ No Capture data only about local hosts
Disable Promiscuous Mode (-s)	○ Yes ◉ No Don't set the interface(s) into promiscuous mode
Run as daemon (-d)	○ Yes ◉ No Run Ntop as a daemon

Save Prefs | Restore Defaults

This is essentially a graphical representation of most of ntop's command line options and the explanations accompanying each option are self explanatory. The noteworthy ones for me are:

- ☑ **Capture Interfaces**: Allows you select which interfaces to capture traffic on. The default is your primary interface i.e. eth0.
- ☑ **HTTP Server**: I choose a different port from the default 3000 – meaning that I access my ntop web UI using http://a.b.c.d:5000
- ☑ **Run as daemon**: When ntop starts, I want it to leave the command line interface and work in the background like other services. If you are having problems and need to see error information as it occurs, you should choose No.

Don't forget to click **Save Prefs** to save you modified configuration. Should you wish to return to ntop's defaults, just click the **Restore Defaults** button. Notice that the screenshot is just one of six possible pages where you can configure start-up preferences. Click on the other links at the top of the page to get to the other pages.

Configure ntop

[Basic Prefs] [**Display Prefs**] [IP Prefs] [FC Prefs] [Advanced Prefs] [Debugging Prefs]

Preference	Configured Value
Refresh Time (-r)	120 Delay (in secs) between automatic screen updates for supported HTML pages
Max Table Rows (-e)	0 Max number of lines that ntop will display on each generated HTML page
Show Menus For	(•) IP ( ) FC ( ) Both
No Info On Invalid LUNs	( ) Yes (•) No Don't display info about non-existent LUNs
Use W3C	(•) Yes ( ) No Generate 'BETTER' (but not perfect) w3c compliant html 4.01 output

Save Prefs | Apply Prefs | Restore Defaults

[Basic Prefs] [Display Prefs] [**IP Prefs**] [FC Prefs] [Advanced Prefs] [Debugging Prefs]

Preference	Configured Value
Use IPv4 or IPv6 (-4/-6)	(•) v4 ( ) v6 ( ) Both
Local Domain Name (-D)	abu.edu.ng Only if ntop is having difficulty determining it from the interface or in case of capture files
No DNS (-n)	( ) Yes (•) No Skip DNS resolution, showing only numeric IP addresses
TCP/UDP Protocols To Monitor (-p)	format is <label>=<protocol list> [, <label>=<protocol list>] OR a filenameof a file containing such a format
P3P-CP	Return value for p3p compact policy header
P3P-URI	Return value for p3p policyref header

Save Prefs | Restore Defaults

Configure ntop

[Basic Prefs] [Display Prefs] [IP Prefs] [FC Prefs] [**Advanced Prefs**] [Debugging Prefs]

Preference	Configured Value
Max Hashes (-x)	30000 Limit number of host hash entries created in order to limit memory used by ntop
Max Sessions (-X)	65353 Limit number of IP sessions entries created in order to limit memory used by ntop
Don't Merge Interfaces (-M)	○ Yes ◉ No Yes = merge data from all interfaces (if possible), No = do not merge data from all interfaces
No Instant Session Purge	◉ Yes ○ No Makes ntop respect the timeouts for completed sessions
Don't Trust MAC Address (-o)	◉ Yes ○ No Situations which may require this option include port/VLAN mirror
Pcap Log Base Path (-O)	/usr/local/var/ntop Directory where packet dump files are created
Use SSL Watchdog	○ Yes ◉ No
Disable SchedYield	○ Yes ◉ No

Save Prefs | Restore Defaults

Configure ntop

[Basic Prefs] [Display Prefs] [IP Prefs] [FC Prefs] [Advanced Prefs] [**Debugging Prefs**]

Preference	Configured Value
Run in debug mode (-K)	○ Yes ◉ No Simplifies debugging Ntop
Trace Level (-t) *(takes effect immediately)*	3 Level of detailed messages ntop will display
Save Other Packets (-j)	○ Yes ◉ No Useful for understanding packets unclassified by Ntop
Save Suspicious Packets (-q)	○ Yes ◉ No Create a dump file (pcap) of suspicious packets
Log HTTP Requests (-a)	Request HTTP logging and specify the location of the log file
Use Syslog (-L)	1 Send log messages to the system log instead of stdout
Write captured frames to (-l)	Causes a dump file to be created of the captured by ntop in libpcap format
Disable Extra Mutex Info	○ Yes ◉ No Disables storing of extra information about the locks and unlocks of the protective mutexes Ntop uses

Save Prefs | Restore Defaults

Tweaking Ntop – Preferences

Access the **Edit Preferences** page by clicking **Admin→Configure→Preferences**. This brings up a page similar to the screenshot shown.

Edit Preferences

Preference	Configured Value	Action
rrd.dataDumpInterval	300	Set
globals.localityPolicy	0	Set
pluginStatus.PDA	0	Set
pluginStatus.Round-Robin Databases	1	Set
ntop.stickyHosts	0	Set
netflow.2.netFlowAggregation	0	Set
rrd.dumpShortInterval	10	Set
rrd.permissions	0	Set
pluginStatus.Host Last Seen	1	Set
rrd.dataDumpDomains	0	Set
globals.displayPolicy	1	Set
pluginStatus.Remote	1	Set
rrd.hostsFilter		Set
rrd.dataDumpMonths	24	Set
ntop.maxNumSessions	65353	Set
rrd.rrdDumpDelay	10	Set
rrd.rrdPath	/usr/local/var/ntop/rrd	Set
		Add

Most of these options can have command line equivalents. Typically, 0 means a parameter is off and 1 means it is on. Other options take directory paths and integers. You set a parameter by typing in its value and clicking the **Set** button. To delete an entry, simply leave its value field blank and then click the **Set** button. The very last row provides space for you to type in parameters that don't exist on the page. This is where you would define host clusters for example.

Common Questions

Don't expect to understand everything about ntop overnight, some things you will figure out only with time. Here are some of the questions I have scratched my head about then finally figured out.

Is There Any Difference Using Ntop to Monitor a LAN versus a WAN?

What do Protocol Decoders Do? Do I Need Them?

From Burton M. Strauss on the ntop mailing lists: protocol decoders examine and collect information about layer 2 protocols such as NetBIOS or Netware SAP, as well as about specific TCP/IP protocols, such as DNS, http and ftp. This support is specifically coded for each protocol and is different from the capability to count raw information (packets and bytes) by protocol specified by the -p | --protocols parameter.

Decoding protocols is a significant consumer of resources. If the ntop host is underpowered or monitoring a very busy network, you may wish to disable protocol decoding either through the Admin→Configure→Preferences page or by using the -b | --disable-decoders parameter of the ntop command. By default, protocol decoders are enabled.

How Do I Designate Hosts as Local or Remote?

By default, all IP addresses in the subnet of the interfaces in the ntop server are considered local and anything else is considered remote. If you have several subnets using different IP address ranges, you may want to take a summary of those and configure them either through Admin→Configure→Startup Options or Admin→Configure→Preferences. In my case for example, because I know all the three different private IP address ranges are being used on the network [a terrible design I must admit ;-(], I designated 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 as local subnets. Anything else is considered remote. Ntop automatically considers all hosts in the IP range of its interfaces as local, so if the IP address on one of your interfaces in your ntop server is 192.168.20.1/24, then that entire subnet – 192.168.20.0/24 is automatically considered local by ntop.

What is the 95th Percentile Thing on Graphs?

The 95th percentile is a widely used mathematical calculation to evaluate regular and sustained utilisation of a network pipe. Its value shows the highest consumption of traffic for a given period. Calculating the 95th percentile means that 95% of the time the usage is below a certain amount, and 5% of the time usage is above that amount. The 95th percentile is a good value to use to show the bandwidth that is actually used at least 95% of the time.

How do I configure port mirroring on a Cisco Switch?

Suppose you want to mirror all traffic entering and leaving port FastEthernet 0/2 to FastEthernet 0/1 [to which you plug in your ntop server] proceed thus:

```
switch#configure terminal
switch(config)#monitor session 1 source interface FastEthernet 0/2 both
switch(config)#monitor session 1 destination interface FastEthernet 0/1
```

The SPAN destination port's line protocol status will change to down state. This is normal behaviour and the computer connected to that port cannot send any traffic that is not related to the SPAN session.

What are Host Clusters and How do I Configure Them?

Host Clusters are a way for you to give a descriptive name to a range of IP addresses that enables you to then monitor traffic statistics for that range as a single entity. For example, suppose I know that the range of addresses 172.16.2.0/24 is exclusively used by guests, then I can define a host cluster called guests that groups all addresses in the range 172.16.2.0/24. From now on, I can get aggregated statistics for how much bandwidth guests are consuming on my network.

To configure them, click **Admin→Configure→Preferences**, then scroll to the last row in the table which provides spaces for you to configure an option and its value. To define a new host cluster, type cluster.<name> in the text box on the left and then type a network list to the right and click on the Add button. For example to define my cluster above, I would type `cluster.Guests` in the left and then `172.16.2.0/24` in the right.

To Trust or Not to Trust MAC Addresses in Ntop

In some ntop reports, you might see the same MAC address listed for several hosts. You need to understand that only MAC addresses on a segment that is local [i.e. in the same broadcast domain] with an interface of ntop can be trusted. A router will typically re-write the layer 2 addressing information, inserting the MAC address of its own interface as the source address which is what you get to see as the source MAC address for various different hosts. There is both a command line parameter [`- o`] as well as an option in the Start-up Options page in the WEBUI that lets you tell ntop not to trust MAC addresses.

References/Sources/Further Reading

1. "Open Source in Network Administration: The ntop Project" by Luca Deri - Presentation made at the 3rd Open Source Conference, Athens, May 2008
2. "Ntop User's Guide" by Luca Deri
3. "Ntop, Persistent Data and RRD" by Burton M. Strauss
4. "Ntop: Beyond Ping and Traceroute" by Luca Deri & Stefano Suin
5. Ntop FAQ by Luca Deri and Burton M. Strauss III
6. "How to Accelerate Your Internet" edited by Rob Flickenger [bmwo.net]