



ntopng User's Guide

Version 2.0

May 2015



Index

Acknowledgements	2
Preface	3
What is ntopng?	3
How to start ntopng?	3
How ntopng works.	8
Home Menu	10
About ntopng	10
ntop Blog	11
Report an Issue	11
Dashboard.....	11
Dashboard	12
Dashboard in the Community Version	12
Dashboard in the Professional Version	17
Report	18
• Flows Menu.....	19
• Hosts Menu.....	21
All Hosts	22
Networks	31
Autonomous Systems.....	32
Countries	32
Operating Systems.....	32
HTTP Server (Local)	33
Aggregations	33
Interactions.....	34
Top Hosts (Local).....	34
Top Hosts Traffic	34
Geo Map	35
Tree Map	36
Local Matrix.....	36
• Protocols Menu.....	36
• Interfaces Menu	37
• Other Menus	41
Setting Menu	41
Administration Menu	44
Alerts Menu	45
Search Host.....	45
Additional ntopng Features.....	46

Acknowledgements

Many thanks to InsideNet Solutions (<http://www.insidenetsolutions.com>) and TruePath technologies (<http://truepathtechnologies.com>) for editing and reviewing this manual.



Preface

By reading this book, you will learn how to install ntopng, how to use the basic elements of the graphical user interface (such as menu bars) and what's behind some of the cool features that are not always obvious at first sight. It will hopefully guide you around some common problems that frequently appear for new (and sometimes even advanced) users of ntopng.

What is ntopng?

Ntopng is a passive network monitoring tool focused on flows and statistics that can be obtained from the traffic captured by the server.

How to start ntopng?

Ntopng can be started from the command line of your favorite Linux, Unix and Windows system. Services control panel are also supported in Windows. When starting ntopng it's possible to modify its behaviour by customising one or more of the several optional settings available, using either the command line, or grouping them in a configuration file used and start ntopng with it.

```
ntopng <configuration file path>
ntopng <command line options>
```

ntopng supports a large number of command line parameters. To see what they are, simply enter the command *ntopng -h* and the help information should be printed:

```
ntopng x86_64 v.2.1.151023 - (C) 1998-15 ntop.org

Usage:
  ntopng <configuration file path>
  or
  ntopng <command line options>

Options:
  [--dns-mode|-n] <mode>                                | DNS address resolution mode
  | 0 - Decode DNS responses and resolve                |
  |   local numeric IPs only (default)                  |
  | 1 - Decode DNS responses and resolve all           |
  |   numeric IPs                                     |
  | 2 - Decode DNS responses and don't                |
  |   resolve numeric IPs                            |
  | 3 - Don't decode DNS responses and don't          |
  |   resolve numeric IPs
  [--interface|-i] <interface|pcap>                      | Input interface name (numeric/symbolic),
  | view or pcap file path                           |
  | Data directory (must be writable).                 |
  | Default: /var/tmp/ntopng
  | Daemonize ntopng
  | HTTP documents root directory.
  | Default: httpdocs
  | Scripts directory.
  | Default: scripts
  | Callbacks directory.
  | Default: scripts/callbacks
  | Don't set the interface in promiscuous mode.
  | Key used to access host categorization
  | services (default: disabled).
  | Please read README.categorization for
  | more info.
```



```
[--httpbl-key|-k] <key>
| Key used to access httpbl
| services (default: disabled).
| Please read README.httpbl for
| more info.

[--http-port|-w] <[:]:http port>
| HTTP port. Set to 0 to disable http server.
| Prepend a : before the port to listen to the
| loopback address. Default: 3000

[--https-port|-W] <[:]:https port>
| HTTPS port. See usage of -w above. Default: 3001

[--local-networks|-m] <local nets>
| Local nets list (default: 192.168.1.0/24)
| (e.g. -m "192.168.0.0/24,172.16.0.0/16")

[--ndpi-protocols|-p] <file>.protos
| Specify a nDPI protocol file
| (eg. protos.txt)

[--disable-host-persistency|-P]
[--redis|-r] <host[:port] [@db-id]>
[--user|-U] <sys user>

[--dont-change-user|-s]
[--shutdown-when-done]
[--disable-autologout|-q]
[--disable-login|-l] <mode>

[--max-num-flows|-X] <num>
| Max number of active flows
| (default: 131072)

[--max-num-hosts|-x] <num>
| Max number of active hosts
| (default: 65536)

[--users-file|-u] <path>
| Users configuration file path
| Default: ntopng-users.conf

[--pid|-G] <path>
| Pid file path

[--disable-alerts|-H]
[--packet-filter|-B] <filter>
[--dump-flows|-F] <mode>
| Disable alerts generation
| Ingress packet filter (BPF filter)
| Dump expired flows. Mode:
|   es      Dump in ElasticSearch database
|   Format:
|     es;<idx type>;<idx name>;<es URL>;<http auth>
|   Example:
|     es;ntopng;ntopng-%Y.%m.%d;http://localhost:9200/_bulk;
|   Note: the <idx name> accepts the strftime() format.
|   mysql  Dump in MySQL database
|   Format:
|     mysql;<host|socket>;<dbname>;<table name>;<user>;<pw>
|       mysql;localhost;ntopng;flows;root;
|   Export flows using the specified endpoint.
|   Dump hosts policy (default: none).
|   Values:
|     all    - Dump all hosts
|     local  - Dump only local hosts
|     remote - Dump only remote hosts
|     none   - Flush hosts when idle
|   Enable hw timestamping/stripping.
|   Supported TS modes are:
|     apcon - Timestamped packets by apcon.com
|             hardware devices
|     ixia  - Timestamped packets by ixiacom.com
|             hardware devices
|     vss   - Timestamped packets by vssmonitoring.com
|             hardware devices
|   Enable tap interfaces used to dump traffic
|   HTTP prefix to be prepended to URLs. This is
|   useful when using ntopng behind a proxy.
|   Check if the license is valid.
|   Check until maintenance is included in the license.
|   Verbose tracing

[--export-flows|-I] <endpoint>
[--dump-hosts|-D] <mode>

[--sticky-hosts|-S] <mode>

--hw-timestamp-mode <mode>

[--enable-taps|-T]
[--http-prefix|-Z] <prefix>

[--check-license]
[--check-maintenance]
[--verbose|-v]
```



```
[--version|-V]           | Print version and quit
[--help|-h]             | Help

Available interfaces (-i <interface index>):
 1. eth0
 2. eth1
 3. eth2
 4. lo0
```

Here we describe some of the most important ones:

```
[--redis|-r] <redis host[:port] [@db-id]>
```

Ntopng uses Redis as a backend database to store user configuration and preferences. Redis must be started before ntopng. By default the location is localhost but this can be changed by specifying host and port where Redis is listening. During startup procedure the connection to a remote Redis database is shown as (*<Timestamp>: Successfully connected to Redis 127.0.0.1:6379@0*). In case the connection can't be established, the following error occurs (*<Timestamp> ERROR: ntopng requires redis server to be up and running*). In case multiple ntopng instances use same Redis server is it important, to prevent data from being overwritten, to specify the “@db-id” (where db-id is a number > 0) string to reserve a single Redis database to every ntopng instance.

```
[--interface|-i] <interface|pcap>
```

At the end of the help information there a list of all available interfaces. The user can select one or more interfaces from the list so that ntopng will treat them as monitored interfaces. Any traffic flowing through monitored interfaces will be seen and processed by ntopng. On Windows systems you will specify the interface number (i.e. -i 1). On Linux / Unix use the interface name. A monitoring session using multiple interfaces can be set up as follows:

```
ntopng -i eth0 -i eth1
```

The following is also allowed:

```
ntopng -i eth0,eth1
```

To specify a zmq interface (more details later on) you should add a configuration like this:

```
ntopng -i tcp://<endpoint ip>/
```

In this case monitored data will be shown as single interface or grouped by aggregation.

Ntopng is also able to compute statistics based on pcap traffic files:

```
ntopng -i /tmp/traffic.pcap
```

```
[--http-prefix|-Z] <prefix>
```

Network admins who want to monitor their network, may want to map ntopng web interface using a reverse proxy. The main issue with reverse proxying is that the ‘/’ URI should not be mapped to the ntopng base. Customizable prefixes for the ntopng base can be chosen using the http-prefix option.

Generally speaking, when the http-prefix is used, ntopng web interface is accessible by pointing the browser at [http://<host>:<port>/<prefix>/](http://<host>:<port>/<prefix>)

For example, ntopng web interface can be accessed at <http://localhost:3000/myntopng> if it is executed as

```
ntopng -Z /myntopng
```



Using Apache, one would achieve the same behavior with the following http proxypass directives:

```
ProxyPass /myntopng/ http://192.168.100.3:3000/myntopng/  
ProxyPassReverse /myntopng/ http://192.168.100.3:3000/myntopng/
```

[--dns-mode|-n] <mode>

This option controls the behavior of the name resolution done by ntopng. User can specify whether to use full resolution, local- or remote-only, or even no resolution at all.

[--data-dir|-d] <path>

Ntopng uses a data directory to store several kinds of information. Most of the historical information related to hosts and applications is stored in this directory. Historical information includes round robin database (RRD) files for each application/host.

[--local-networks|-m] <local nets>

Ntopng characterizes networks in two categories, namely local and remote. Consequently, also hosts are characterized in either local or remote hosts. Every host that belongs to a local network is local. Similarly, every host that belongs to a remote network is remote.

Local networks are ‘special’ for ntopng. Indeed, it stores much more information (e.g., layer-7 protocols) for local networks if compared to their remote counterparts. However, additional information comes at the cost of extra memory and space used. Therefore, although a user would virtually want to mark all possible networks as local, in practice he/she will have to find a good tradeoff.

Local networks can be specified as a comma separated list of IPv4 (IPv6) addresses and subnet masks. For example to mark three networks as local ntopng can be executed as follows:

```
ntopng -local-networks="192.168.2.0/24,10.0.0.0/8,8.8.8.0/24"
```

In the ntopng web interface, local networks and hosts are displayed with green colors while remote networks and hosts hosts with gray colors. Extra information will be available in the contextual menus for local networks.

[--disable-login|-l]

By default ntopng uses authentication method to access the web GUI. Authentication can be disabled by adding the option disable-login to the startup parameters. In this case any user who access the web interface has administrator privileges.

As mentioned above, a configuration file can be used in order to start ntopng. Below is an example of configuration file used to start ntopng:

```
# cat /tmp/ntopng.conf  
-g=-1  
-A=2  
-E=local  
-D=local  
-S=local
```



```
-C  
-G=/var/tmp/ntopng.pid  
-i=eth0
```

Warning

Unlike its predecessor, ntopng is not itself a Netflow collector. It can act as Netflow collector combined with nProbe. To perform this connection start nProbe with the “--zmq” parameter and point ntopng interface parameter to the nProbe zmq endpoint. Using this configuration give the admin the possibility to use ntopng as collector GUI to display data either from nProbe captured traffic and Netflow enabled devices as displayed in the following picture.

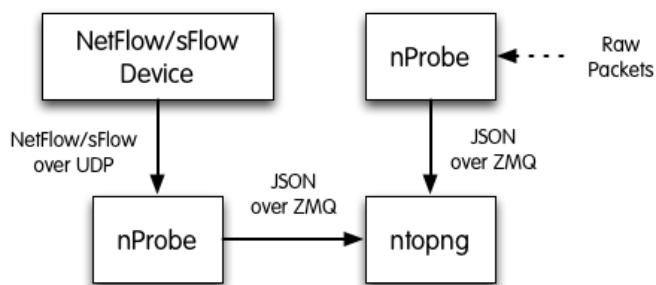


Figure 1 - ntopng/nprobe setup

Keep in mind that even if logically nProbe is a ntopng client, the session starts the other way around (ntopng connects to nprobe endpoint), hence in case of firewalled connection, the flow is initiated by ntopng



How ntopng works.

After ntopng has started you can view the GUI. By default, the GUI can be accessed from any web browser at `http://<ntopng IP>:3000/`. A different port can be specified as a command line option during ntopng startup. The first page that always pops out contains the login form — provided that the user has not decided to turn authentication off during startup.

If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.

© 1998-2015 - ntop.org
ntopng is released under GPLv3.

Hint: the default user and password are admin

The Login Page

The default login is

username	admin
password	admin

Administrator privileges are granted to user ‘admin’.

If an unauthenticated user attempts to access a specific ntopng URL, the system will redirect the browser to the login page and then, upon successful authentication, to the requested resource.

Ntopng GUI web pages have a common structure the user will soon be familiar with. The pages are mostly composed of a top toolbar, some body content, and a ‘dashboard’ footer.

The main toolbar appears as follows.



The Header Bar



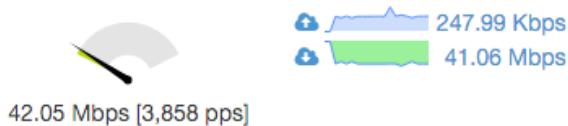
The items list are *Home*, *Flows*, *Hosts*, *Protocols*, *Interfaces*, *Setting*, *Logout*, and *Search Host*. An extra item *Alert* pops out when some alerts fired in reaction of user configuration.

In the left part of the footer, ntopng summarizes some information such as logged-in user, monitored interfaces, and used version (Community or Professional).

© 1998- 2015 - ntop.org
Generated by ntopng Professional v.2.1.151023
for user [admin](#) and interface [en4](#)

The Left Side of the Footer Bar

In the center it is shown a gauge which provides the bandwidth saturation level for monitored interfaces. The same information is also reported as a function of time in two dynamic graphs, for upstream and downstream traffic, respectively.



The Center of the Footer Bar

Gauge scale is calculated according to physical interfaces features. It is not always possible to determine maximum nominal interfaces speed. For this reason, scale can me manually configured simply by clicking on the gauge. Changes will be automatically saved to persistent storage.

Finally, in the right side of the footer there is the uptime information, direct links to current Alerts (if any), Hosts, Aggregations, and Flows counters monitored by ntopng.

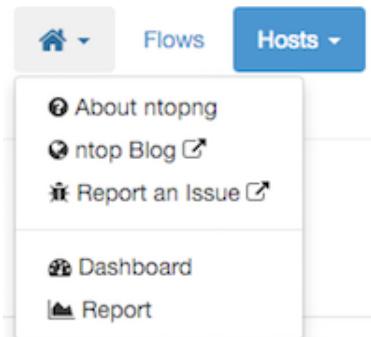
Uptime: 51 min, 30 sec
 2 Alerts 49 Hosts 49 Flows

The Right Side of the Footer Bar

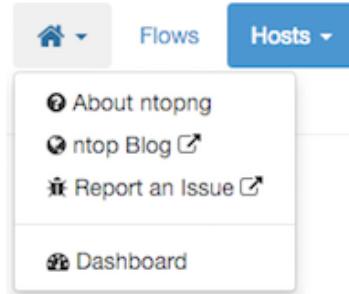


Home Menu

Four items belong to the *Home* menu. An additional entry ‘Report’ is available in the Professional version.



Professional Version Home Menu



Community Version Home Menu

About ntopng

Shows information about ntopng Version, Platform, Currently Logged User, Uptime value and some details related to its internals.

About ntopng

Copyright	© 1998-2015 - ntop.org
License	EULA SystemId: 125E71C2000007F9 [] Click on the above URL to generate your professional version license, purchase a license at e-shop, or mail us for a free evaluation license.
Version	24FCFFEE14BF4ADEF272527550C591E9311460564450CC [Save License]
Platform	1.99.150420 (r9258) - Professional Edition
Currently Logged User	Debian wheezy/sid (x86_64)
Uptime	admin
	1 day, 32 min, 34 sec
NDPI	r1.5.2 (e66b440d35:20150420)
Twitter Bootstrap	3.x
Font Awesome	4.x
RRDtool	1.4.7
Redis Server	2.2.12
Mongoose web server	3.7
LuaJIT	LuaJIT 2.0.3
ØMQ	3.2.4
GeoIP	1.4.8
Data-Driven Documents (d3js)	This product includes GeoLite data created by MaxMind. 2.9.1 / 3.0
Compressed Bitmap (EWAHBoolArray)	0.4.0

The ‘About ntopng’ Page

Need to update the following information:

The upgrade from Community to Professional Version can be done by clicking on the system ID. The browser will be redirected to the ntop shop to generate a valid license. The generated id should be save in the appropriate field in “License” field.



ntop Blog

is a link to <http://www.ntop.org/blog/> page where some useful information of tricks can be found.

Report an Issue

is a link to <https://svn.ntop.org/bugzilla/> page where you can report specific bug you discovered.

Dashboard

Provides a shortcut to default dashboard page of ntopng. The dashboard is discussed in greater detail in the following section.

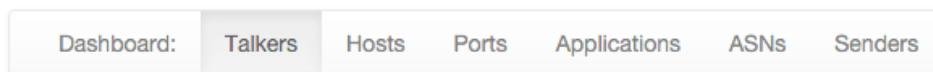


Dashboard

Dashboard is a dynamic page and provides an updated snapshot of the current traffic for the selected interface or interface view being monitored by ntopng. Community and Professional version have two different dashboards.

Dashboard in the Community Version

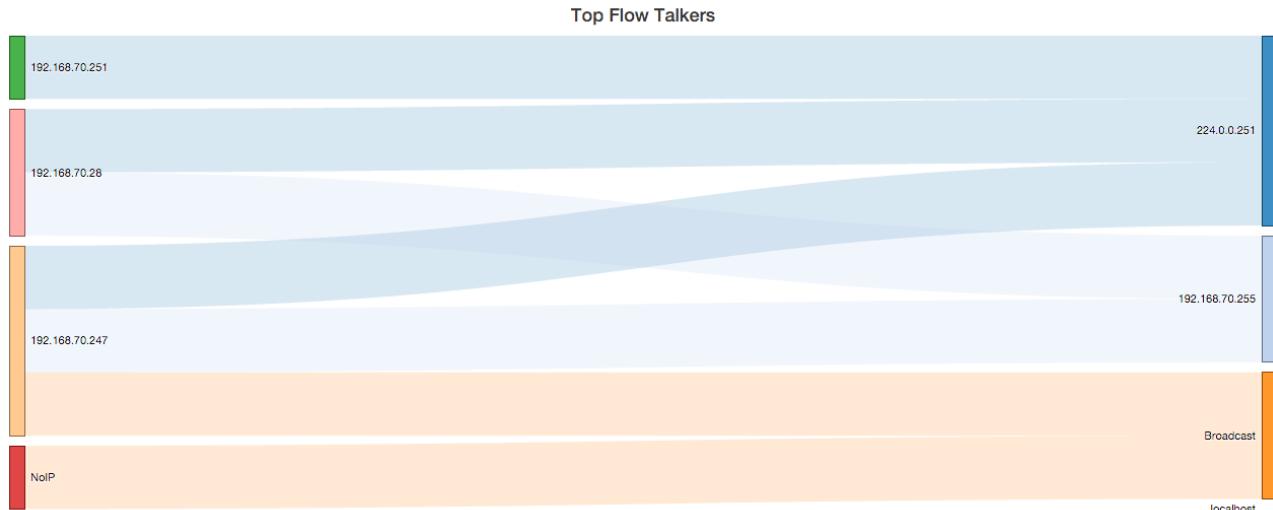
The dashboard provides information about Talkers, Hosts, Ports, Applications, ASNs, and Senders. Information can be selected from the top menu. Each item is discussed below.



The Top Menu for the Dashboard

Talkers

The default dashboard page is a Sankey diagram of Top Flow Talkers



The Sankey Diagram of Top Flow Talkers

Refresh frequency: 5 Seconds Live update:

Diagram Refresh Settings

The Sankey diagram displays hosts currently active on the monitored interface or interface view. Host pairs are joined together by colored bars representing flows. The client host is always placed in the left edge of the bar. Similarly, the server is placed on the right. Bar width is proportional to the amount of traffic exchanged. The wider the bar, the higher the traffic exchanged between the corresponding pair of hosts.

By default, the diagram is updated every 5 seconds. Refresh frequency can be set or disabled from the dropdown menu shown right below the diagram.

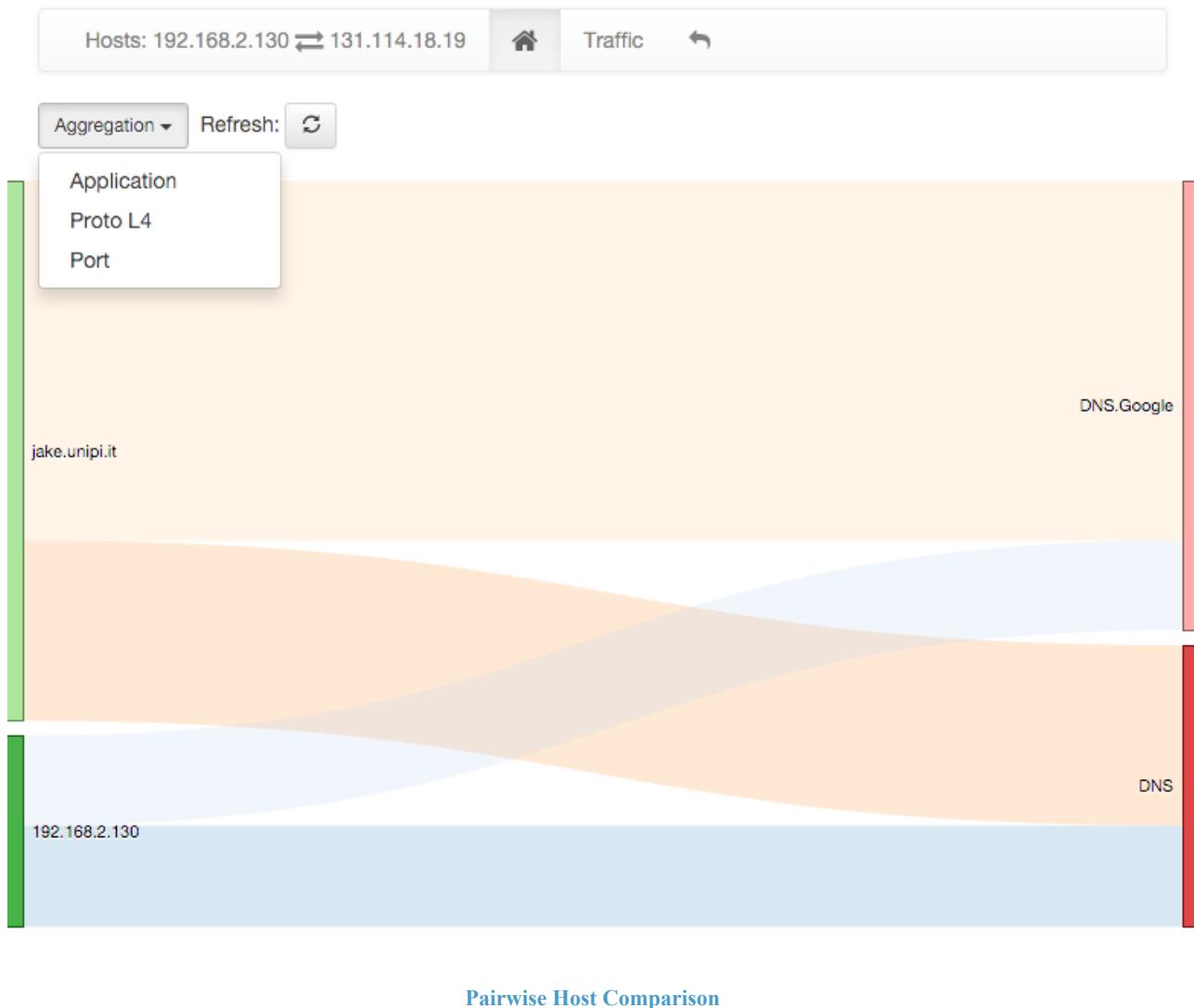


Host and flow information shown in the Sankey is interactive. Indeed, both host names (IP addresses) as well as flows are clickable.

A *double-click* on any host name redirects the user to the ‘Host Details’ page, that contains a great deal of host-related information. This page will be discussed later in the manual.

Similarly, a *double-click* on any bar representing a flow redirects the user to the ‘Hosts Comparison’ page. Hosts can be pairwise compared in terms of Applications, Layer-4 Protocols, and Ports. A pie chart of exchanged traffic can be shown as well.

Below is shown an Application comparison between two hosts. The diagram shows that both hosts on the left have used DNS services (on the right). It is also possible to visually spot behaviors and trends. For example it is possible to see that jake.unipi.it is much more prone to use Google’s DNS than the other host.

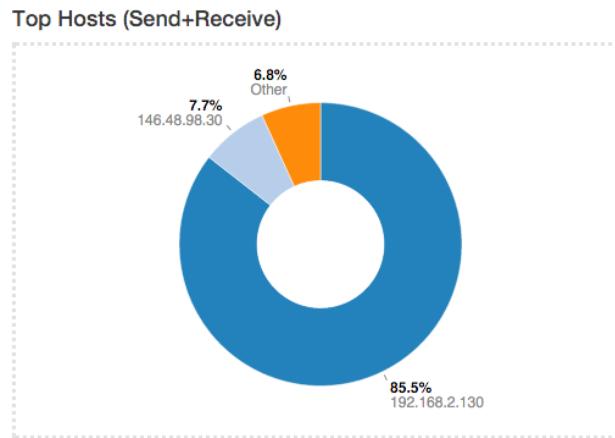




Hosts

Hosts View provides a pie chart representation of the captured traffic. Aggregation is done on a per-host basis. Similarly to the Sankey Diagram discussed above, any host name (or non-resolved IP address) shown can be double-clicked to visit the corresponding ‘Host Details’ page.

The pie chart is refreshed automatically.

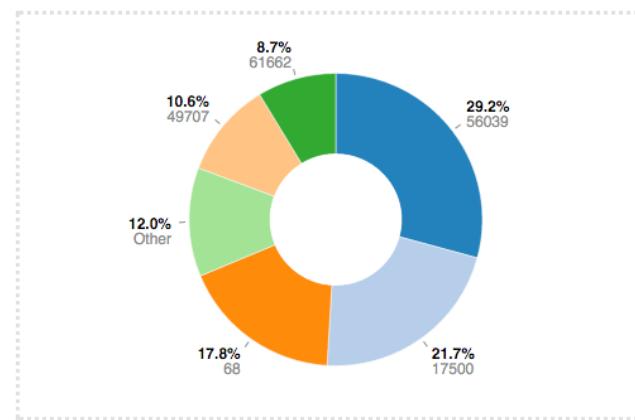


Pie Chart of Top Hosts

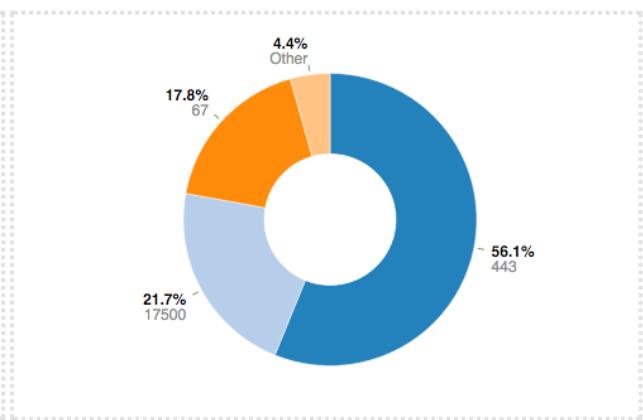
Ports

Ports view provides two separated pie charts with the most used ports, both for clients and for servers. Each pie chart provides statistics for client ports and server ports.

Top Client Ports



Top Server Ports



Pie Chart of Top Client and Server Ports

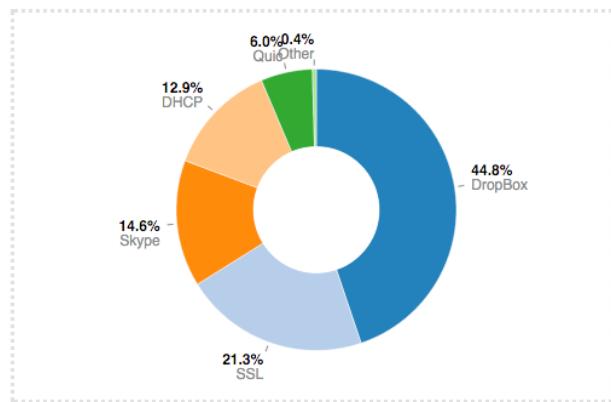
Any port number shown can be double-clicked to visit the ‘Active Flows’ page. This page lists all the currently active flows such that client or server port matches the one clicked.



Application

Application View provides another pie chart that represents a view of the bandwidth usage divided per application protocol. Protocol identification is done through ntop nDPI engine. Protocols that cannot be identified are marked as Unknown.

Top Application Protocols



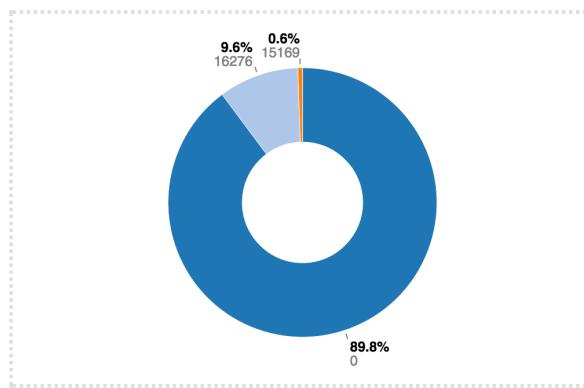
Pie Chart of Top Applications

In the same manner as for previous view, application names are clickable to be redirected to a page with more detailed information on application.

Autonomous System Numbers (ASNs)

ASNs view provides a pie chart representation of the traffic grouped by Autonomous System (AS). An AS is either a single network or a group of networks, controlled by a network administrator on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). An AS is also sometimes referred to as a routing domain. A globally unique number called an Autonomous System Number (ASN) is assigned to each AS.

Top Talker ASNs



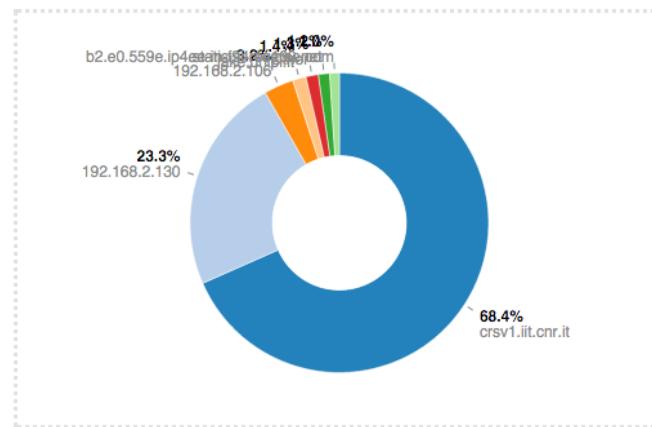
Pie Chart of Top ASNs



Senders

Senders view provides a pie chart representation of top flow senders currently active. This graph shows the percentage of traffic being sent by endpoints either on local or remote networks.

Top Flow Talkers: Live

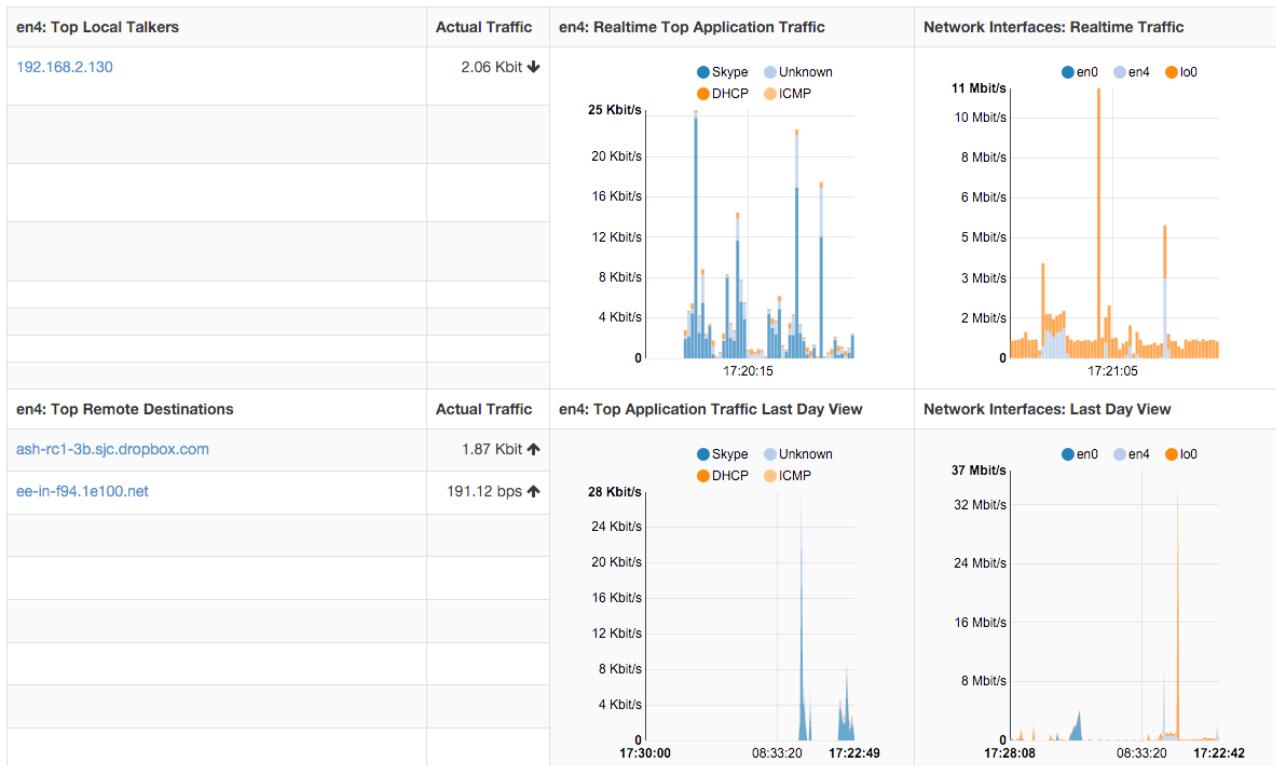


Pie Chart of Top



Dashboard in the Professional Version

The dashboard in the professional version provides a great deal of information, including realtime traffic — both per monitored interface and per application — top local talkers and top destinations. The dashboard is refreshed dynamically. Tables and charts are kept updated by ntopng.



The Dashboard in the Professional Version

The right part of the dashboard displays realtime and last-day charts of Top Applications and Network Traffic. In case a network interface view is selected, then network traffic is shown on a per physical-interface basis. Items shown in each chart can be dynamically toggled simply by clicking on the corresponding colored dot in the chart key.

The left part of the dashboard shows tables of realtime Top Local Talkers and Top Remote Destinations, including the amount of traffic exchanged.

Top Local Talkers are hosts, belonging to local networks, that are exchanging the highest traffic volumes.

Similarly, *Top Remote Destinations* are hosts, belonging to remote networks, that are currently exchanging the highest traffic volumes.

Next to each Actual Traffic value there is an arrow that point up or down. **TODO: Explain the meaning of this arrow.**

Each host show can be clicked to access its ‘Host Details’ page.

TODO: is this feature still present (The badge displayed close to the hostname provides the number of different virtual hosts linked to the ip)?



Report

The Professional Version of ntopng is able to show graphs and tables containing traffic and application statistics and trends.

Using the header bar it is possible to select the time granularity and the type of graphs and tables to be reported.

The screenshot shows the ntopng interface with a header bar. The 'ntop' logo is at the top left. To its right are navigation links: Home, Flows, Hosts, Protocols, Interfaces, Settings, User, and a search bar labeled 'Search Host'. Below the header are two date/time input fields: 'Start Date/Time' set to 2015/04/27 09:56 and 'End Date/Time' set to 2015/04/28 09:56. Between these fields are buttons for 'Update', a checkmark icon, and a lock icon.

Report Menu Pro Version

Header bar contains:

- time granularity 1h (one hour), 1d (one day), 1w (one week), 1M (one month), 6M (six months), 1Y (one year),
- time period start/end date and time,
- filtering: where user can select how filter to apply.



Figure 21 - Filter Option

By clicking the button the following popup menu is displayed where it is possible to select one or more interface (or all) and one or more protocols (or all).

The screenshot shows a 'Filter Report' modal window. It has two main sections: 'Network Interfaces' and 'Protocols'. In 'Network Interfaces', there is a checkbox for 'Toggle All' and one for 'eth0' which is checked. In 'Protocols', there is a checkbox for 'Toggle All' and several other checkboxes for specific protocols: DHCP (checked), HTTP (checked), ICMP (unchecked), ICMPv6 (checked), MDNS (checked), SSH (checked), Skype (checked), and Unknown (unchecked). At the bottom of the modal is a blue 'Submit Filter' button.

Figure 22 - Filter Modal

- print/export pdf data report



Figure 23 - Print Button

Note: filters and preferences are on user basis, hence modifying any of those from different browser sessions may change the expected results in the active session.
By selecting this button, report can be printed.

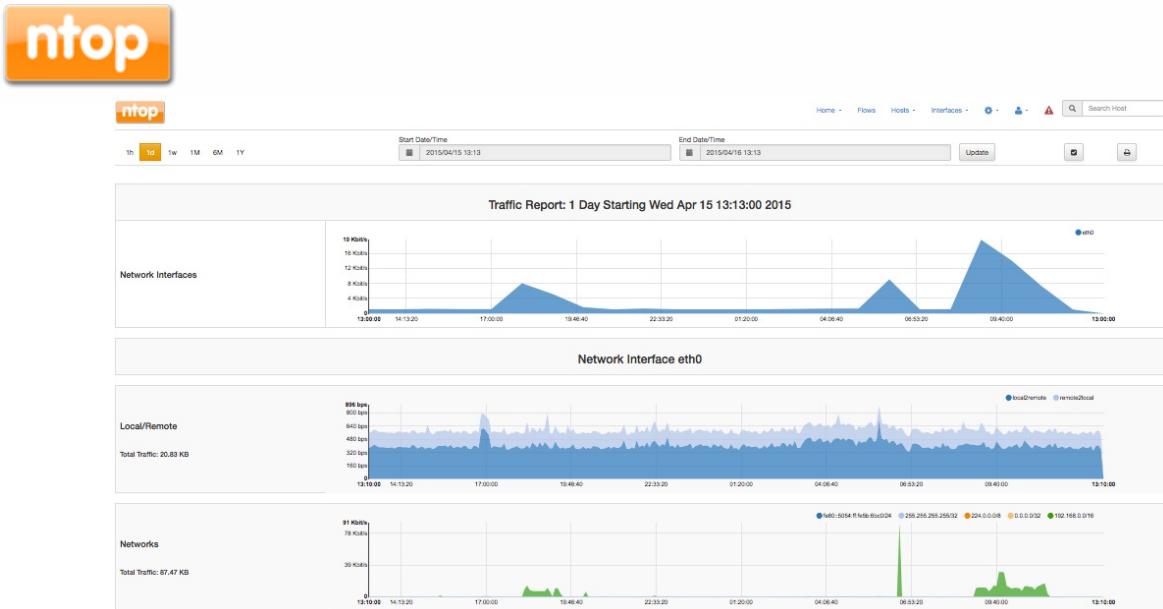


Figure 24 - Report Page Pro Edition

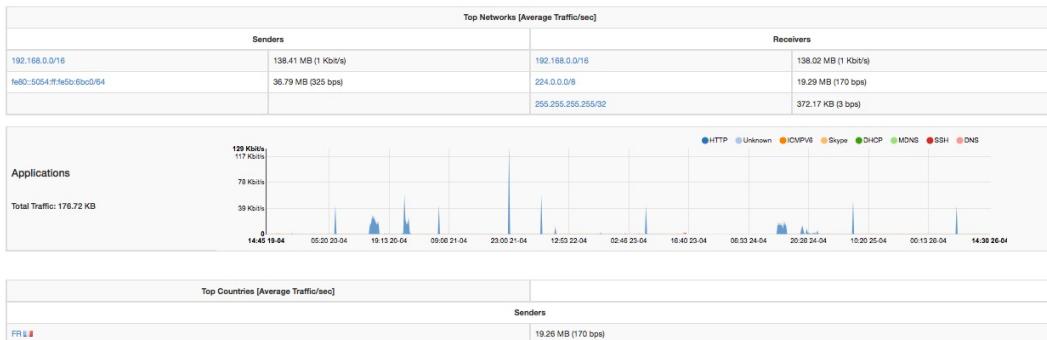


Figure 25 - Report Page Pro Edition Footer

The main content of the page instead contains the graphs on the NIC's overall traffic, the local vs remote traffic, the traffic divided by networks and by applications. The network traffic is also available in table format.

The print button opens a new page with the requested data and the system printing wizard.

• Flows Menu

The next menu item appears as follows and provides the flows/traffic currently active. The number of items to be displayed per page (minimum is 10) and an application filter (default all proto) can be applied (using the appropriate dropdown menu) to adjust the view the preferred way. In addition you can sort all items (ascending / descending / unsorted order) by clicking on Column Name.

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
[Info]	Unknown	UDP	94.23.249.252 [!] :3222	224.0.1.102:3222	23 days, 1 h, 26 min, 30 sec	Client	0 bps —	19.45 MB	
[Info]	Unknown	UDP	94.23.249.253 [!] :3222	224.0.1.102:3222	23 days, 1 h, 26 min, 26 sec	Client	0 bps ↓	19.43 MB	
[Info]	Unknown	UDP	fe80::12bd:18ff:fee4... [!] :2029	ff02::66:2029	23 days, 1 h, 26 min, 12 sec	Client	0 bps —	14.02 MB	
[Info]	ICMPv6	IPv6-ICMP	fe80::ee30:91ff:fee0... [!] :1	ff02::1:ff00:1	6 days, 23 h, 52 min, 58 sec	Client	412.76 bps ↑	9.42 MB	
[Info]	Unknown	UDP	fe80::ee30:91ff:fee0... [!] :2029	ff02::66:2029	23 days, 1 h, 26 min, 22 sec	Client	0 bps ↓	9.29 MB	
[Info]	ICMPv6	IPv6-ICMP	fe80::12bd:18ff:fee4... [!] :1	ff02::1:ff00:1	4 days, 1 h, 35 min, 58 sec	Client	0 bps ↓	5.26 MB	
[Info]	Unknown	UDP	94.23.249.252 [!] :1985	224.0.1.102:1985	23 days, 1 h, 25 min, 58 sec	Client	0 bps —	4.16 MB	
[Info]	HTTP	TCP	ubuntu:80776	192.168.100.5 [!] :3000	24 sec	Client	0 bps ↓	976 Bytes	/ntopng/lua/network_load...
[Info]	HTTP	TCP	ubuntu:55349	192.168.100.5 [!] :3000	24 sec	Client	3.31 Kbit/s ↑	1.27 KB	/ntopng/lua/get_flows_da...
[Info]	HTTP	TCP	ubuntu:64904	192.168.100.5 [!] :3000	1 sec	Client	1.03 Kbit/s ↑	834 Bytes	/ntopng/lua/network_load...

Showing 1 to 10 of 11 rows

Figure 26 - Flows Menu

A flow is identified as a communication between two systems. To simplify the concept of flow, this can be imagined as a communication between a specific protocol from IP A:port X to IP B:port Y. Flows are handled in different manner if TCP or UDP. Thanks to the DPI detection engine included (nDPI), ntopng is able to recognise the used protocol based on the captured traffic (works just with raw packet capture). In case that the DPI engine won't detect a protocol, the system will mark the flows as unknown whereas, if detected, the application name and a thumb (indicating the characterisation of the flow – good/bad traffic). The *Info* button brings the user to a page like the following one, where a detailed report of the flow is available.

Flow Peers	192.168.1.92 [!] :54949 → 93-62-150-157.ip23.fastwebnet.it:443
Protocol	TCP / SSL
First / Last Seen	30/05/2015 17:15:05 [1 min, 5 sec ago] / 30/05/2015 17:16:07 [3 sec ago]
Total Traffic Volume	Nan undefined —
Client vs Server Traffic Breakdown	192.168.1.92:54949 / 93-62-150-157.ip23.fastwebnet...:443
Network Latency Breakdown	19.278 ms (server)
Client to Server Traffic	undefined Pkts / Nan undefined —
Server to Client Traffic	undefined Pkts / Nan undefined —
SSL Certificate	webmail.rcslab.it
TCP Flags	FIN, SYN, PUSH, ACK This flow is completed and will soon expire.
Actual / Peak Throughput	316.42 bps — / 316.42 bps
Dump Flow Traffic	□ ↗

Figure 27 - Flow Details

L4 Prot: this column provides the protocol used in the flow such as UDP, TCP and so on; **Client/Server:** these fields describe host and port involved client or server side. If the host has a public ip address, ntopng shows the country flag for the belonging country. These data are based on MaxMind databases. A blue flag is drawn if the host is the ntopng host. Clicking on the host IP, ntopng provides all information about that host (redirecting the user to the Host Info Page); instead, selecting the port value it is possible to obtain all active flows on that port.



Duration: this describes how long the flow is active;

Breakdown: this describes “data direction”. If you read for instance “client” it means that most of the traffic for that flow is done in the client-to-server direction.

Actual Thpt: this describes current flow throughput (there is a graphical indicator that shows the trend compared to the previous check);

Total Bytes: gives the total amount of traffic of flow, since its activity started.

Info: when ntopng detects an application protocol uses this field to add some value added information (i.e. if protocol is DNS the query, in case of http could be the requested url).

As said for most of ntopng pages, also this contains all the data updated every second.

Network graph, first/last switch (flow time duration is calculated), traffic trend (stable/increasing/decreasing), total volume of traffic and all the other interesting metrics are update every seconds without reloading the page. In this page we have the possibility to know current traffic for both directions client/server.

Application column: when ntopng discovers the used application, this information is provided and, if the application allows, additional application metadata are provided (eg: with http flows). By selecting the application value, ntopng will redirect users to a view with all the hosts creating the requested traffic.

• Hosts Menu

Menu Hosts contains several menu items as shown below.

All Hosts

IP Address	Location	Alerts	Name	Seen Since	ASN	Category	Breakdown	Throughput	Traffic
192.168.1.92	Local	0	192.168.1.92	2 min, 40 sec			S Rcvd	103.06 Kbit/s ↑	7.76 MB
31.13.86.8	Remote	0	edge-star-shv-01-mxp1.facebook...	1 min, 15 sec	Facebook, Inc.		Sent Rcvd	0 bps	8.66 KB
194.132.168.2	Remote	0	lon6-accesspoint-a14.lon6...	1 min, 42 sec	Spotify Technology SARL		Sent ↑	0 bps	117.99 KB
131.114.18.19	Remote	0	jake.unipi.it	2 min, 2 sec	Consortium GARR		Sent Rcvd	0 bps	60.1 KB
17.172.100.8	Remote	0	17.172.100.8	2 min, 16 sec	Apple Inc.		Sent Rcvd	0 bps	21.3 KB
191.239.203.8	Remote	0	blob.am3prdstr10a.store.core...	1 min, 42 sec	Microsoft Corporation		S Rcvd	0 bps	305.66 KB
93.62.150.157	Remote	0	93-62-150-157.ip23.fastwebnet...	2 min, 2 sec	Fastweb SpA		Sent Rcvd	0 bps	127.24 KB
108.160.169.49	Remote	0	ash-ra1-3a.sjc.dropbox.co...	2 min, 1 sec	Dropbox, Inc.		Sent Rcvd	0 bps	4.38 KB
5.178.42.162	Remote	0	5.178.42.162	24 sec	TELECOM ITALIA SPARKLE S.p.A.		Sent	0 bps	6.49 MB
173.194.40.25	Remote	0	mil02s06-in-f25.1e100.ne...	1 min, 19 sec	Google Inc.		Sent Rcvd	0 bps	56.73 KB

Showing 1 to 10 of 30 rows

« < 1 2 3 > »

Figure 28 - Hosts Menu

- *Host*: shows the active hosts;
- *Network*: shows all networks where hosts belong to;
- *Autonomous Systems*: it shows all autonomous systems under monitoring activity;
- *Countries*: based on the information provided by MaxMind databases, the active countries are displayed
- *Operating Systems*: using passive fingerprinting ntopng tries to detect the OS of a specific host
- *HTTP Server (Local)*: it shows monitored HTTP Virtual hosts (local hosts only)
- *Aggregations*: provides data based several aggregation methods for the monitored hosts
- *Interactions*: it shows an interactive graph showing the hosts and their interaction (traffic)
- *activity (network)*



- *Top Hosts Traffic*: it shows traffic of top hosts in order to typology selected;
- *Geo Map*: it shows hosts a report on a geographic map
- *Tree Map*: it shows a tree representation of monitoring environment;
- *Local Matrix*: it shows matrix representation of local systems.

All Hosts

This menu item shows all monitored hosts.

The screenshot shows the 'All Hosts' page of the ntop interface. At the top, there is a navigation bar with links for Home, Flows, Hosts (which is currently selected), Protocols, Interfaces, and other monitoring metrics. A search bar is also present. Below the navigation, the title 'All Hosts' is displayed, followed by a table with 10 rows of host information. The table has columns for IP Address, Location, Alerts, Name, Seen Since, ASN, Breakdown, Throughput, and Traffic. Each row provides detailed statistics for a specific host, including its location (Local or Remote), the number of alerts, its name (including OS icon if detected), the time since it was first seen, its Autonomous System Number (ASN), and its traffic breakdown between send and receive. The throughput and traffic values are shown in both bps and MB. At the bottom of the table, there is a note indicating 'Showing 1 to 10 of 22 rows' and a small navigation bar with page numbers 1, 2, 3, >, and <.

IP Address	Location	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.168.100.5	Local	9	192.168.100.5 🚨 ①	1 day, 23 h, 37 min, 51 sec		Rcvd	8.55 Kbit/s ↓	26.19 MB
192.168.100.1 🍏	Local	9	ubuntu 🚨	1 day, 23 h, 37 min, 51 sec		Sent	8.55 Kbit/s ↓	18.35 MB
192.168.100.2	Local	0	192.168.100.2	1 day, 9 h, 15 min, 55 sec		Sent	0 bps —	7.84 MB
f02::1:ff00:1	Remote	0	#f02::1:ff00:1	1 day, 23 h, 37 min, 51 sec		Rcvd	412.8 bps ↑	5.45 MB
fe80::12bd:18ff:fee4:5040	Local	0	fe80:12bd:18ff:fee4:504... 🚨	1 day, 23 h, 37 min, 48 sec		Sent	0 bps —	4.49 MB
224.0.0.102	Local	0	224.0.0.102	1 day, 23 h, 37 min, 50 sec		Rcvd	0 bps ↓	3.71 MB
fe80::ee30:91ff:fee0:dfc0	Local	0	fe80:ee30:91ff:fee0:dfc... 🚨	1 day, 23 h, 37 min, 51 sec		Sent	412.8 bps ↑	3.57 MB
94.23.249.252	Remote	0	94.23.249.252 🇫🇷	1 day, 23 h, 37 min, 48 sec	OVH	Sent	0 bps ↓	2.12 MB
f02::66	Remote	0	#f02::66	1 day, 23 h, 37 min, 48 sec		Rcvd	0 bps —	2.01 MB
94.23.249.253	Remote	0	94.23.249.253 🇫🇷	1 day, 23 h, 37 min, 50 sec	OVH	Sent	0 bps ↓	1.76 MB

Figure 29 - All Hosts Page

The table is made of several columns where the following information are provided:

- ip address – with the icon of the OS if detected
- location (either remote or local)
- alerts – the number of alerts associated to the host
- name – the resolved hostname or the friendly name, the flag of the location of the server (in case of public ip address) and eventually the alert symbol (in case of active alerts for the hosts)
- Seen Since – the amount of time from the first packet seen from/to the host
- ASN – autonomous system (if available)
- Breakdown – send/receive activity
- Throughput – overall actual throughput for the host
- Traffic – total traffic moved by the host

As Flows List, all Column Names are clickable in order to sort hosts list. Clicking on the ip address, a detailed page for the host is displayed as follows:

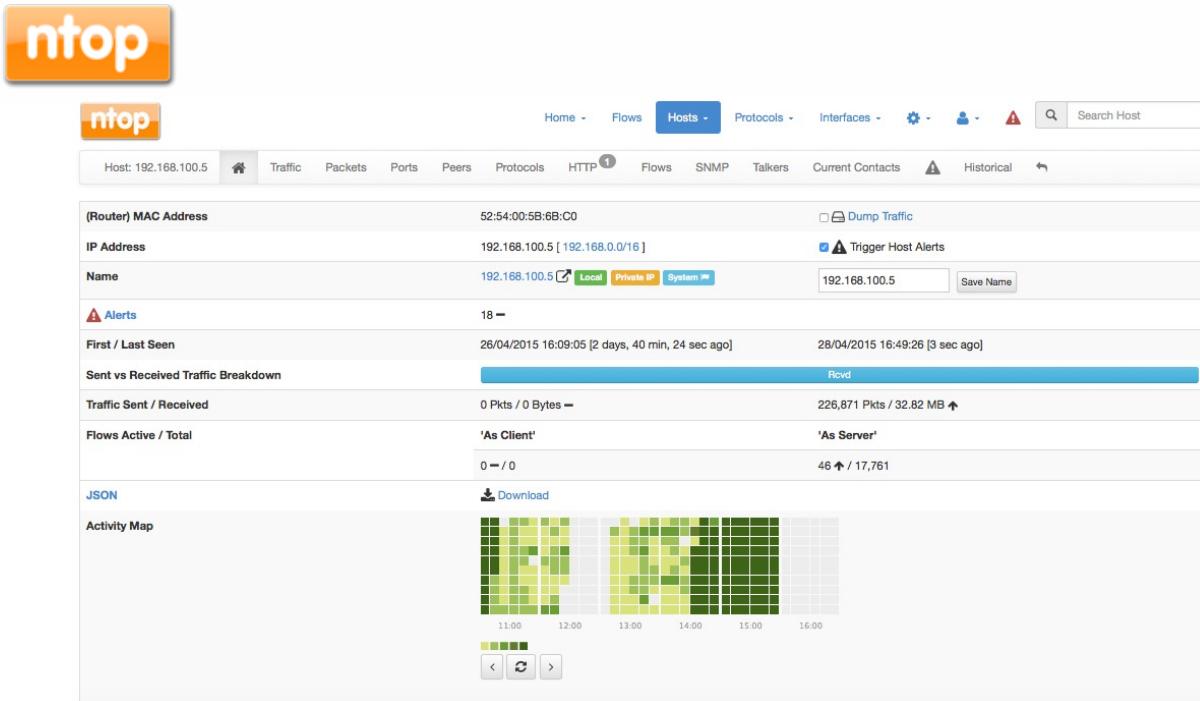


Figure 30 - Host Details Main Page

Host Page provides an additional menu containing a few custom specific views.



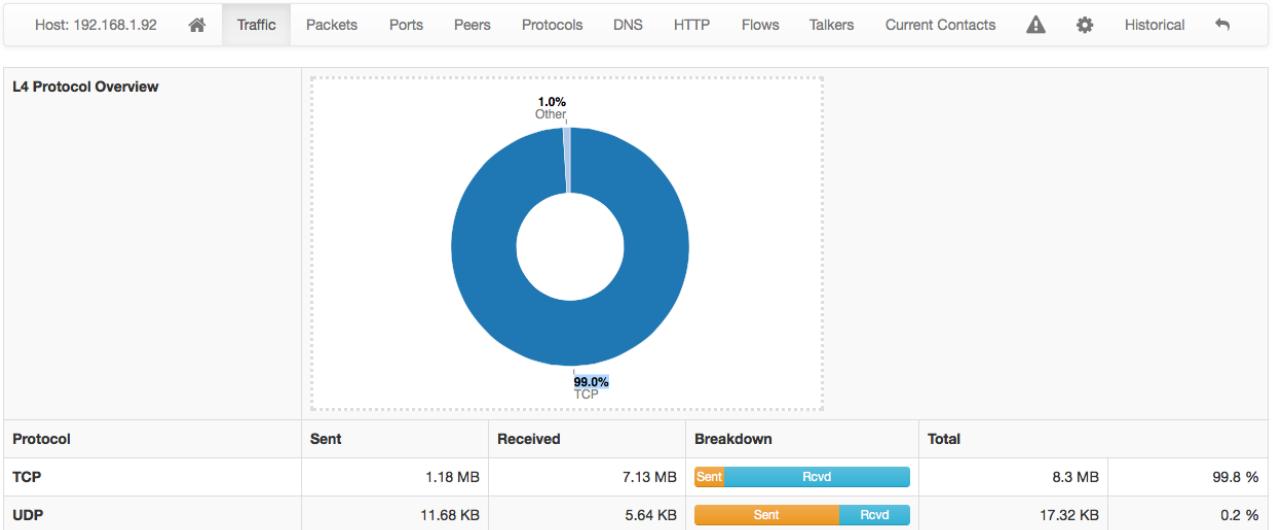
Figure 31 - Host Header Bar

Menu items are dynamic, hence, some of them may not appear:

- **Home (icon):** it provides several generic information such as MAC Address (or last Router Address when is a remote host), IP Address (with network mask if detected), a toggle to activate/deactivate alerts for the host and a trigger to enable packet dump for the specific host, the hostname (if resolved) and some info as local/remote location, private IP or System. It is possible to specify a custom name for each host. Date and time of first and last packet seen for the host, traffic breakdown, amount of traffic packets received/sent, number of flows as client/server host. All of this information is also available in JSON format by clicking on the appropriate link. The heat map provides the Activity Map for each host. Each box represents one minute of traffic for the host. This Activity Map shows last six hours monitored, but it is possible to scroll back to visualize previous values. The darker the green, the higher the traffic produced by the host, compared with the overall



traffic.



- **Traffic:** this page provides layer 4 traffic statistics for the host either in pie chart and

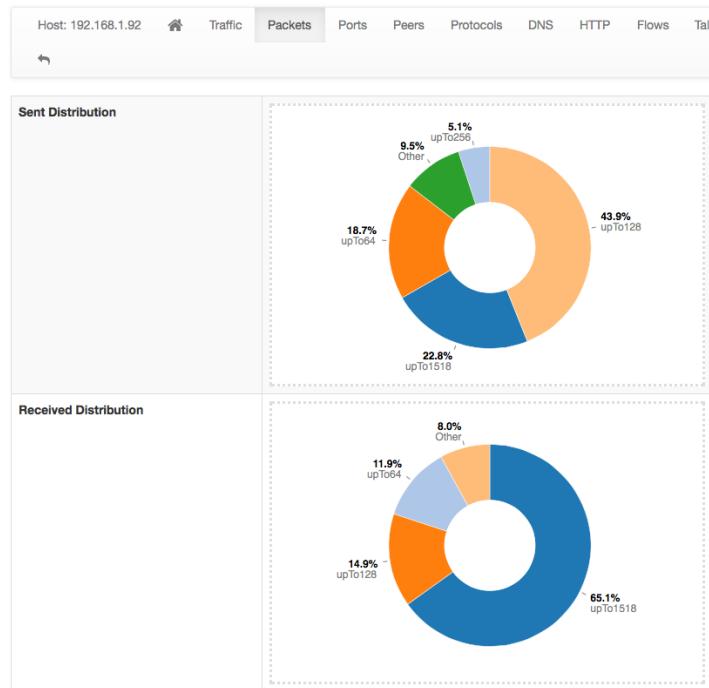


table format.

Figure 32 - Host Layer 4 View

Counters are available for each traffic protocol.

- **Packets:** this page provides a pie chart with the packet size distribution.

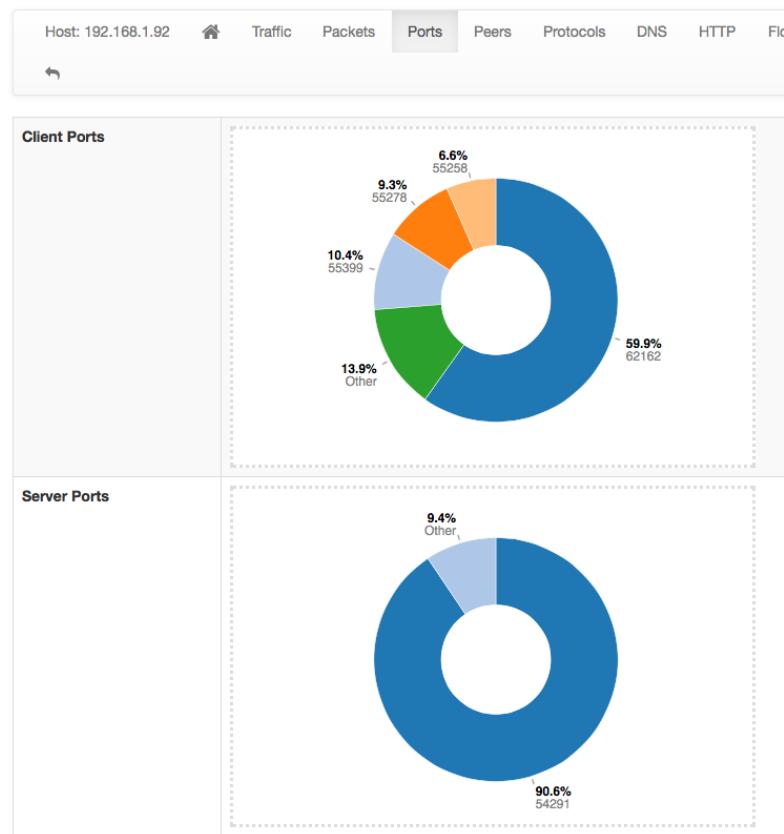


Figure 33 - Host Packets View

- **Ports:** provides a pie chart with the traffic statistics grouped by port. A chart is available for client ports and another one is available for server ports;

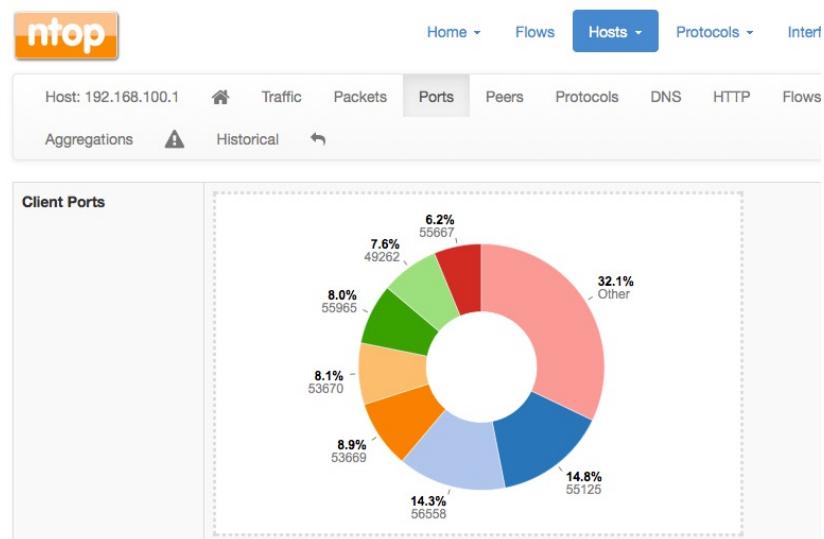


Figure 34 - Host Ports View

- **Peers:** graphical overview of top contacted peers and top protocol used;

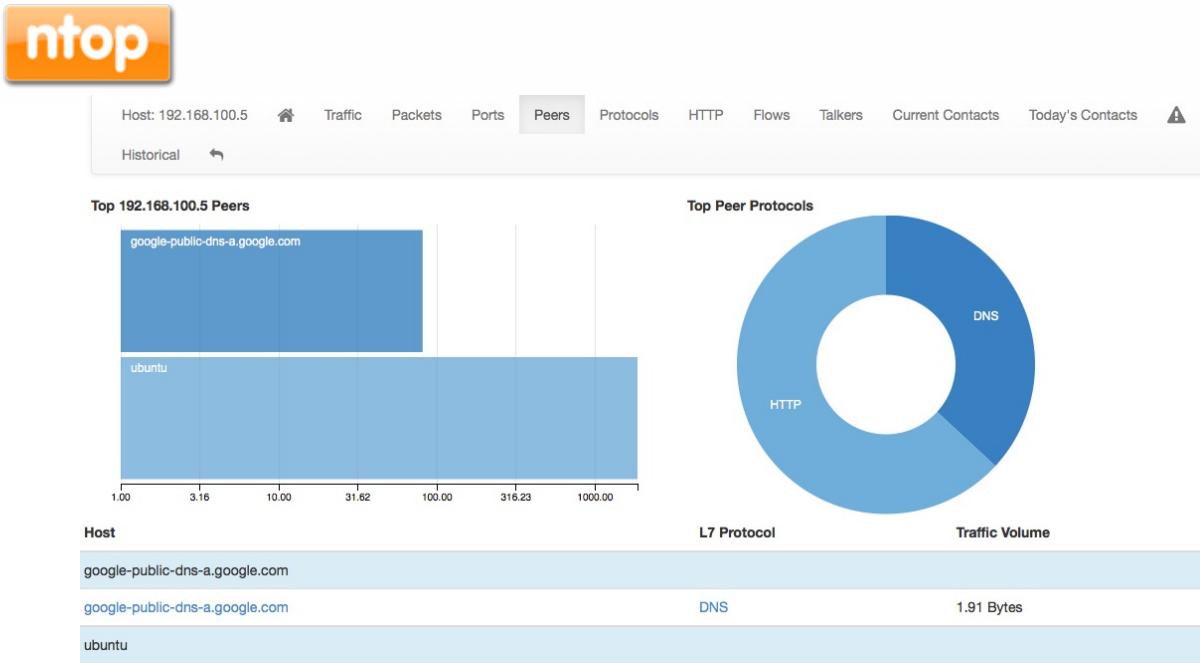


Figure 35 - Host Peers View

Hosts displayed in the table are clickable to drill down further and that will bring up the page for that specific host.

- **Protocol:** using the DPI information, this page provides in pie chart format and tabular format the amount of traffic divided by application. An additional pie chart provides a statistics about protocol type. Each protocol has an icon close to the protocol name where it is displayed the categorisation of protocol (e.g. an acceptable protocol has a thumb up icon);



Figure 36 - Host Protocols View

Clicking on the protocol name, will redirect the user to the page with the detailed statistics about the selected protocol.

- **DNS:** the chart and the table displayed on this page reports protocol specific statistics. Such as the number of queries, type of queries, errors and other DNS related stats are reported.

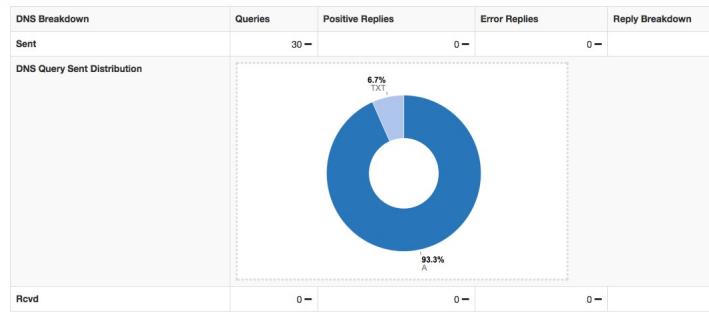


Figure 37 - Host DNS View

- **HTTP:** this page provides information about the HTTP protocol in terms of requests done and responses received for each type of HTTP method used and the response code returned. ntopng provides counters in a table and pie chart representation. In the case of virtual host being detected, a badge with the number of virtual hosts detected for the same IP address is displayed in the host bar and an entry for each virtual server is displayed in the virtual server table section as displayed in the following pictures.

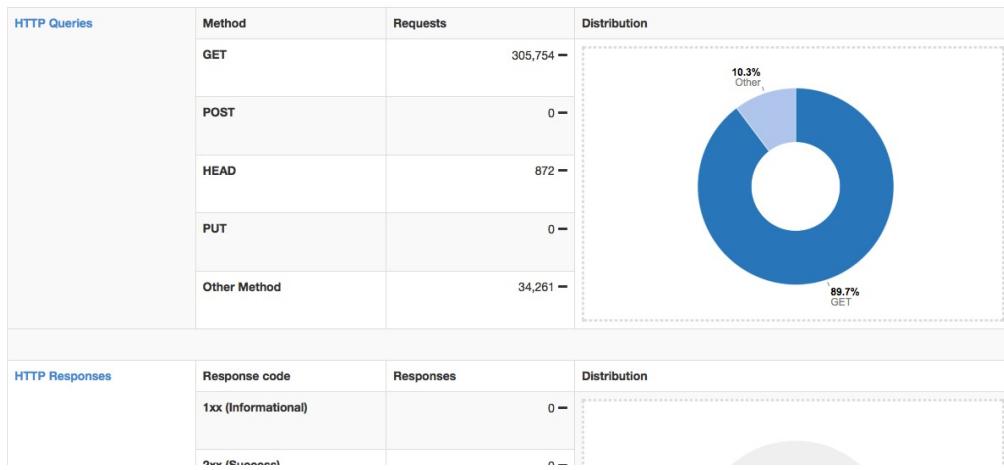


Figure 38 - Host HTTP Header View

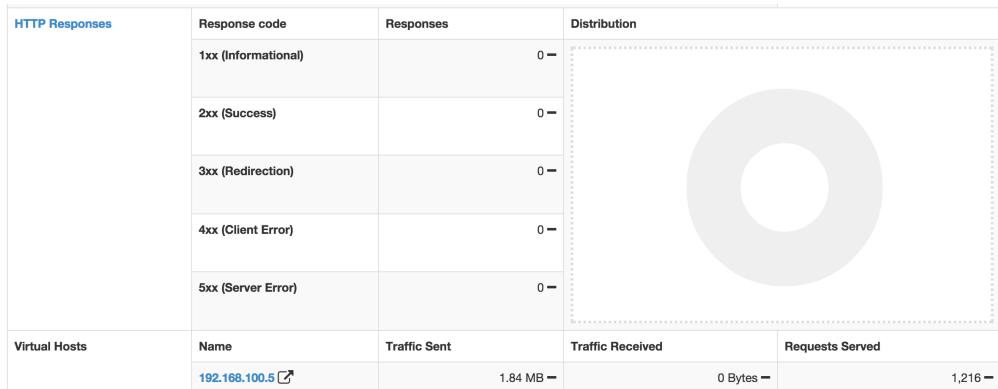


Figure 39 - Host HTTP Footer View

- **Flows:** this page provides all active flows that involve a host.
- **SNMP:** this page provides SNMP information for the selected host with all the standard SNMP traffic metrics.

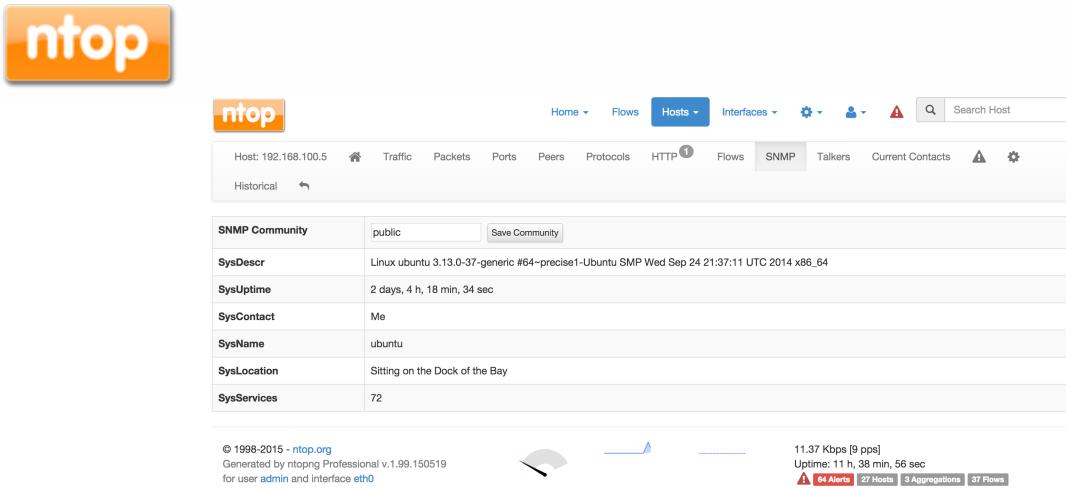


Figure 40 - Host SNMP View

- **Talkers:** this page provides the top talkers with active flows with selected host. This is structured as the Dashboard, filtered by the selected hosts.

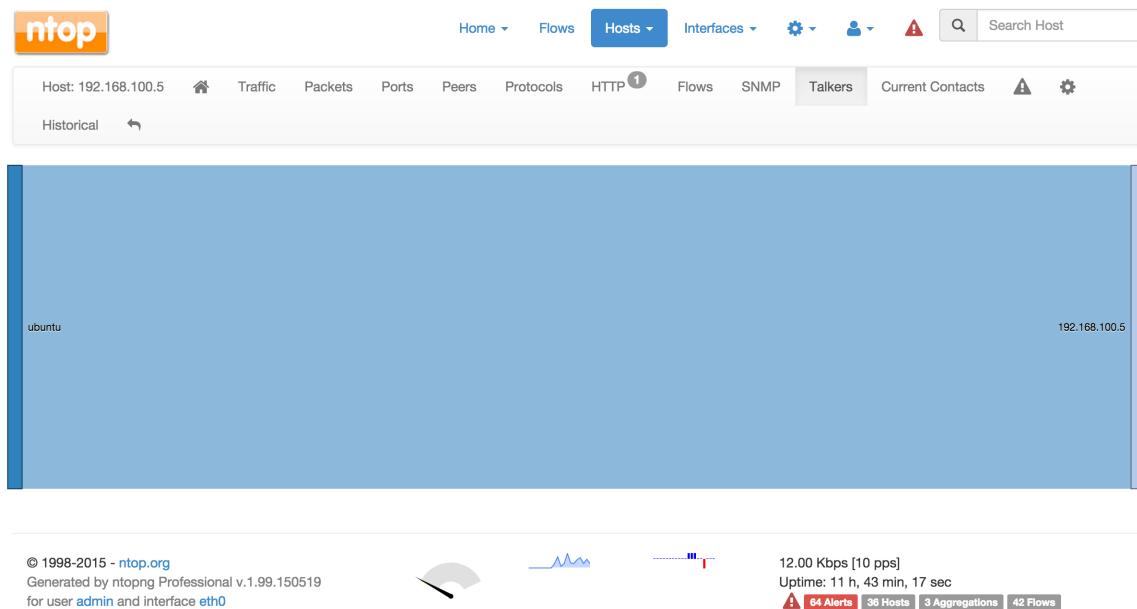


Figure 41 - Host Talkers View

- **Geomap (icon):** this page provides a map where host is located. In this case Ntopng will request the host location to the client browser and, in order to display the host pin, user must allow the localization

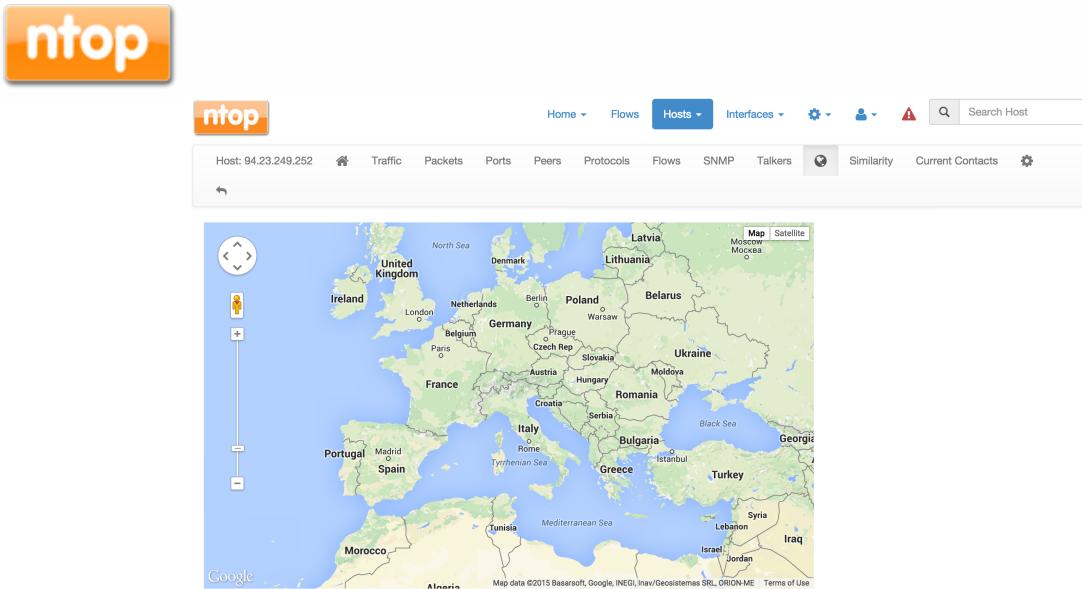


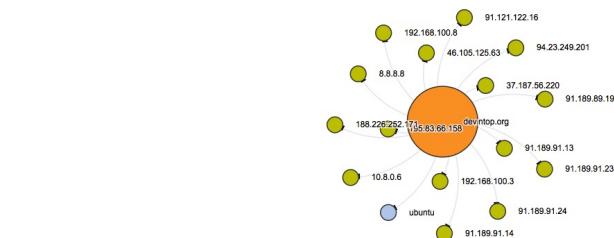
Figure 42 - Host Geo Location View

- **Similarity:** this page display the list of the host defined “similar” in terms of traffic done. Similarity uses the Jaccard Coefficient (http://en.wikipedia.org/wiki/Jaccard_index)



Figure 43 - Host Similarity View

- **Current Contact:** this page provides a graphical representation of all connections (contacts) for that host. In a specific table some statistics about how many times the selected host has been contacted by each client:



NOTE

1. This map is centered on host **devntop.org**. Clicking on this host you will visualize its details.
2. Color map: local, remote, aggregation, focus host.
3. Click is enabled only for hosts that have not been purged from memory.

Figure 44 - Host Contacts View



Client Contacts (Initiator)		Server Contacts (Receiver)	
	No client contacts so far	Client Address	Contacts
		ubuntu	356,620
		8.8.8	25,628
		46.105.125.63	1,218
		91.121.122.16	1,215
		37.187.56.220	1,214
		91.189.89.199	1,211
		195.83.66.158	1,198
		192.168.100.8	872
		10.8.0.8	110

Figure 45 - Host Contacts Table

- *Today's Contacts*: this page provides a daily statistic report of all contacts established by this host. All information in this page is available in JSON format.

Figure 46 - Host Daily Contacts

- *Aggregations*: aggregation view provides a view of clients for that host.

Client Host Aggregations

10 - Aggregations-					
Name	Protocol	Aggregation	Seen Since	Last Seen	Query Number
ntop.org	HTTP	Domain Name	24 min, 40 sec	1 sec	2,193 ↓
Intel Mac OS X 10.10	Unknown	Operating System	24 min, 40 sec	1 sec	2,193 ←

Showing 1 to 2 of 2 rows

Figure 47 - Host Clients Aggregation View

- *Alert Configuration (icon)*: by selecting this menu item we can select threshold values when to generate an alert. Thresholds can be set per total bytes, DNS traffic, P2P traffic or packets delta computed in an alarm interval (minute/5 minutes/hourly/daily).

Host: 192.168.1.92

Traffic
Packets
Ports
Peers
Protocols
DNS
HTTP
Flows
Talkers
Current Contacts

Historical

Every Minute	Every 5 Minutes	Hourly	Daily										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 5px;">Alert Function</th> <th style="text-align: left; padding: 5px;">Threshold</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">bytes</td> <td style="padding: 5px; text-align: center;"> <input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Bytes delta (sent + received) </td> </tr> <tr> <td style="padding: 5px;">dns</td> <td style="padding: 5px; text-align: center;"> <input type="button" value="> <"/> <input style="width: 100px;" type="text"/> DNS traffic delta bytes (sent + received) </td> </tr> <tr> <td style="padding: 5px;">p2p</td> <td style="padding: 5px; text-align: center;"> <input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Peer-to-peer traffic delta bytes (sent + received) </td> </tr> <tr> <td style="padding: 5px;">packets</td> <td style="padding: 5px; text-align: center;"> <input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Packets delta (sent + received) </td> </tr> </tbody> </table>				Alert Function	Threshold	bytes	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Bytes delta (sent + received)	dns	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> DNS traffic delta bytes (sent + received)	p2p	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Peer-to-peer traffic delta bytes (sent + received)	packets	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Packets delta (sent + received)
Alert Function	Threshold												
bytes	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Bytes delta (sent + received)												
dns	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> DNS traffic delta bytes (sent + received)												
p2p	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Peer-to-peer traffic delta bytes (sent + received)												
packets	<input type="button" value="> <"/> <input style="width: 100px;" type="text"/> Packets delta (sent + received)												
Save Configuration Delete All Host Configured Alerts]													

Figure 48 - Host Alert Configuration View

- *Historical*: this page provides historical traffic statistics done by the host. The historical window starts from last 5 minutes to the last year. User can choose to filter the statistics on a protocol basis and display data in several formats (bytes/packets/flows...)



Figure 49 - Host Historical View



Figure 50 - Host Historical DropDown View Menu

Networks

menu item shows all networks discovered by ntopng.

Network Name	Hosts	Alerts	Seen Since	Breakdown	Throughput	Traffic
192.168.0.0/16	6	0	5 days, 2 h, 2 min, 32 sec	Sent Rcvd	12.23 Kbit/s	82.67 MB
Unknown network	3	0	5 days, 2 h, 2 min, 31 sec	Sent Rcvd	428.8 bps	14.99 MB
224.0.0.0/8	2	0	5 days, 2 h, 2 min, 31 sec	Rcvd	0 bps	9.7 MB
fe80::5054:ff:fe5b:6bc0/24	2	0	5 days, 2 h, 2 min, 29 sec	Sent	428.8 bps	5.87 MB
255.255.255.255/32	1	0	5 days, 1 h, 5 min, 22 sec	Rcvd	0 bps	342.4 KB

Showing 1 to 5 of 5 rows

Figure 51 - Host Networks Page



For each network discovered ntopng provides the number of hosts, alerts triggered, date of discovery, breakdown, throughput and traffic. Network name value can be selected to display the hosts list inside the network selected. Clicking on the network name, a page will appear with all the hosts belonging to the selected network.

Autonomous Systems

menu item shows all autonomous systems discovered by ntopng.

The screenshot shows the 'Autonomous Systems' page. At the top, there is a navigation bar with links for Home, Flows, Hosts (selected), Protocols, Interfaces, settings, users, and search. Below the navigation bar is a table titled 'Autonomous Systems' with the following data:

AS number	Hosts	Alerts	Name	Seen Since	Breakdown	Throughput	Traffic
0	12	0	Private ASN	5 days, 2 h, 3 min, 52 sec	Sent Rcvd	13.29 Kbit/s ↓	103.91 MB
16276	2	0	OVH ↗ ITI	5 days, 2 h, 3 min, 51 sec	Sent	96 bps ↑	9.84 MB

Below the table, it says 'Showing 1 to 2 of 2 rows'.

Figure 52 - Hosts AS Page

ntopng uses a Maxmind database to gather information about Autonomous Systems (AS) and based on this info it will group hosts belonging to the same AS. For instance on the figure shown above we have 2 hosts that are belonging to autonomous systems named OVH, this is the reason ntopng is able to aggregate statistics for both hosts to AS number #16276. AS number #0 is a set when all hosts belong to private autonomous systems network.

Countries

this page provides all countries discovered in traffic by ntopng.

The screenshot shows the 'Hosts by Country' page. At the top, there is a navigation bar with links for Home, Flows, Hosts (selected), Protocols, Interfaces, settings, users, and search. Below the navigation bar is a table with the following data:

Name	Hosts	Alerts	Seen Since	Breakdown	Throughput	Traffic
FR	2	0	4 days, 6 h, 34 min, 37 sec	Sent	0 bps —	8.13 MB
US	1	0	1 h, 5 min, 22 sec	Sent	0 bps —	27.39 KB

Below the table, it says 'Showing 1 to 2 of 2 rows'.

Figure 53 - Hosts Countries Page

It is possible to select a Country Name value to show all hosts belonging that country.

Operating Systems

Host list filtered by OS if it was detected.

Name	Hosts	Alerts	Seen Since	Breakdown	Throughput	Traffic
Intel Mac OS X	1	0	4 days, 6 h, 33 min, 1 sec	Sent	9.98 Kbit/s	554.67 MB

Showing 1 to 1 of 1 rows

Figure 54 - Hosts Operating System Page

It is possible to select Operating System Name value to show all hosts with that OS.

HTTP Server (Local)

All Local HTTP Server hosts.

HTTP Virtual Host	HTTP Server IP	Bytes Sent	Bytes Received	Total Requests	Actual Requests
192.168.100.5	192.168.100.5	28.02 MB	28.04 MB	0 Bytes	23,539

Showing 1 to 1 of 1 rows

Figure 55 - Hosts Local HTTP Servers Page

By selecting HTTP Server IP value users will be redirected to the virtual server specified by the HTTP virtual host field. Several different Virtual hosts may refer to the same http server ip and this is the reason why also the server ip is specified in the closed column. Additional info as bytes sent/received are available for each http virtual host. By clicking magnifying lens icon on HTTP virtual host value you can display all active flows where that host is involved.

Aggregations

this page provides all aggregations established by ntopng.

Name	Protocol	Aggregation	Seen Since	Last Seen	Query Number
ntop.org	HTTP	Domain Name	37 min, 46 sec	1 sec	4,305 ↑
ubuntu.com	DNS	Domain Name	21 min, 41 sec	1 min, 1 sec	23 ←
Intel Mac OS X 10.10	Unknown	Operating System	37 min, 46 sec	1 sec	4,305 ←

Showing 1 to 3 of 3 rows

Figure 56 - Hosts Aggregation Page



Aggregations page provide a table with all the hosts grouped based on different criteria, such as operating system, domain name, operating system, and so on

Interactions

this page provides all interactions available among all the hosts monitored by ntopng. Clicking on an item will redraw the graph with the selected host as the central item.

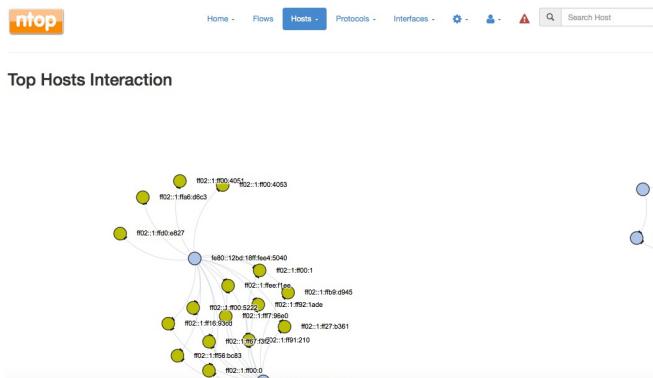


Figure 57 - Hosts Interactions Page

Top Hosts (Local)

This page provides current hosts activity on time basis. If the page is kept the graph will be updated in real time with the freshly collected data of each host. The time scale is divided each 5 minutes and began from time of observation.

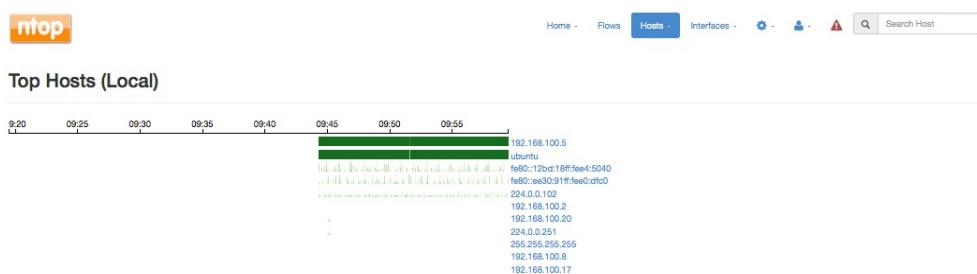


Figure 58 - Hosts Top Local Hosts Page

Top Hosts Traffic

This page provides a traffic matrix with a heat map. The darker the color and the higher is the traffic done by those hosts.

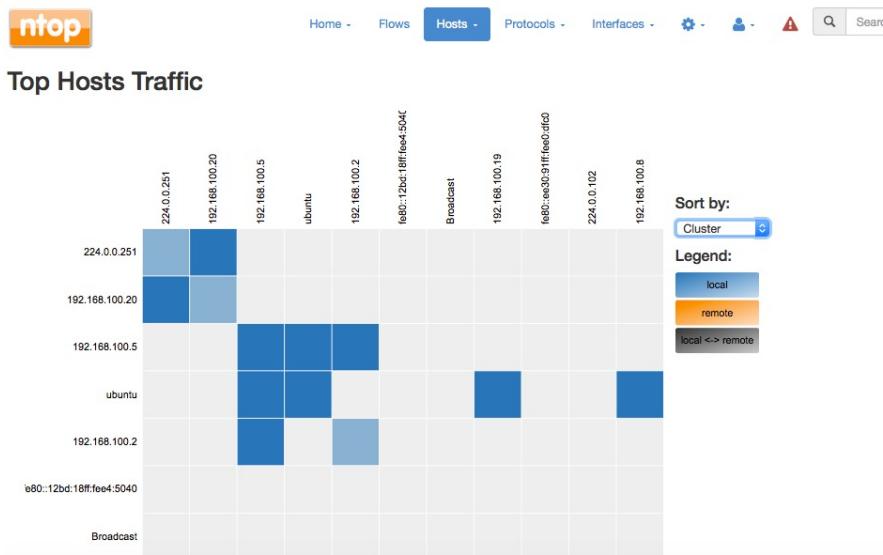


Figure 59 - Hosts Top Traffic Hosts Page

It is possible to establish several sorting criteria: Name, Frequency, Cluster, Traffic Sent, Traffic Rcvd and Total Traffic.



Figure 60 - Hosts Top DropDown Traffic Menu

Geo Map

This page provides world map where hosts are located

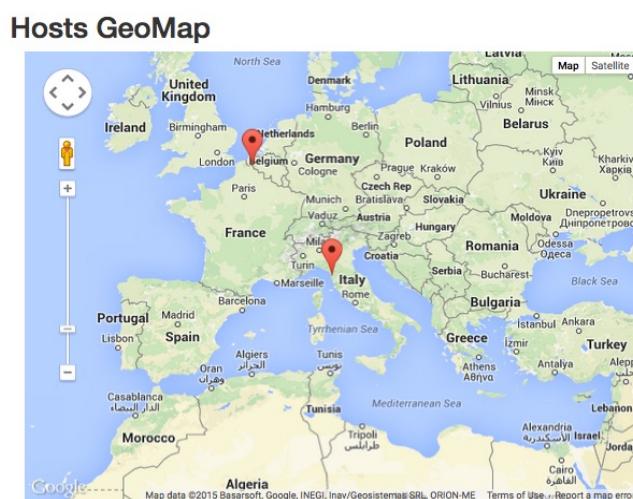


Figure 61 - Hosts Geomap Page



Tree Map

This page provides a tree map of all hosts monitored. By selecting host value you can display all host information in an appropriate page.

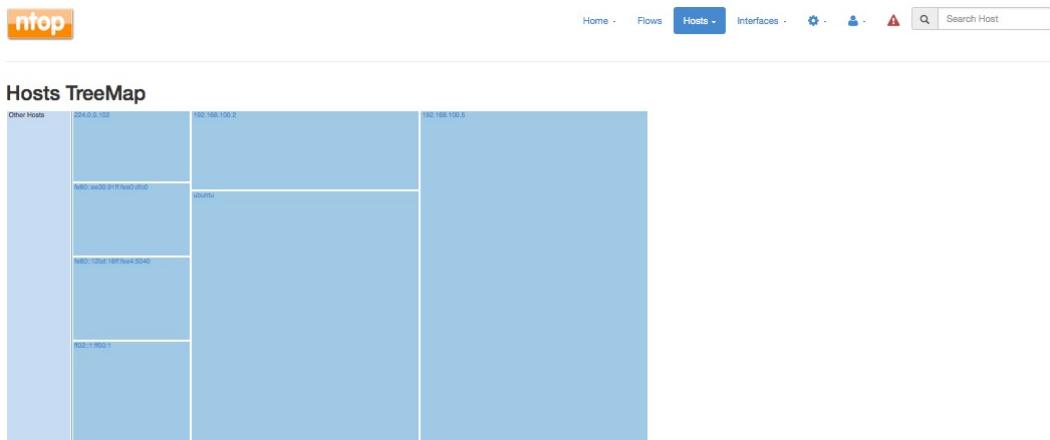


Figure 62 - Hosts TreeMap Page

Local Matrix

This page provides a matrix based on the traffic done by the hosts. It is related just to the hosts marked as local by ntopng and this could be used to detect how traffic flows between local hosts

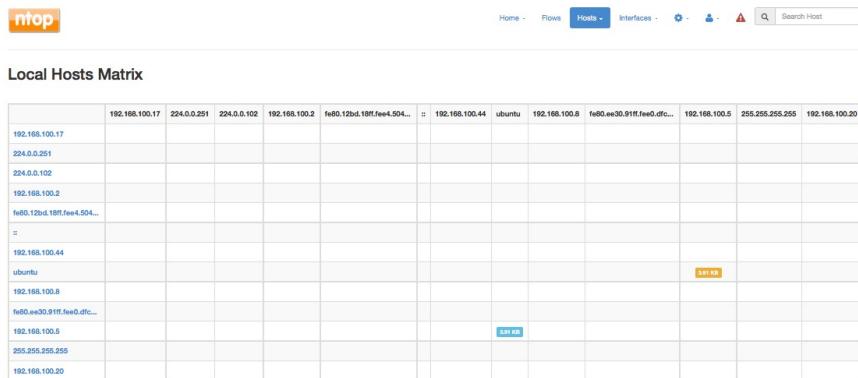


Figure 63 - Hosts Local Matrix Page

• Protocols Menu

Menu Protocols contains menu item for each active protocol (i.e. we have DNS only in the figure below).

Figure 64 - Protocols Menu

When you select a protocol, a new page will be shown with all information for that protocol. For instance for DNS we will have the following page where ntopng will list all DNS queries submitted.

The screenshot shows the ntop web interface. At the top, there's a navigation bar with links for Home, Flows, Hosts, Protocols (which is currently selected), Interfaces, Settings, and User. A search bar labeled 'Search Host' is also present. Below the navigation, the title 'DNS Queries' is displayed. A table lists one entry: 'ubuntu.com' under 'Name', 'DNS' under 'Protocol', 'Domain Name' under 'Aggregation', '13 min, 22 sec' under 'Seen Since', '3 sec' under 'Last Seen', and '12' under 'Query Number'. A note at the bottom says 'Showing 1 to 1 of 1 rows'.

Figure 65 - Protocols DNS Page

• Interfaces Menu

Interfaces contains dropdown menu to select one of the interfaces configured in ntopng that is listening to traffic (i.e. eth0 and eth1 in the figure below) and historical menu item. Historical menu item is enabled if you have to started ntopng with -F option.

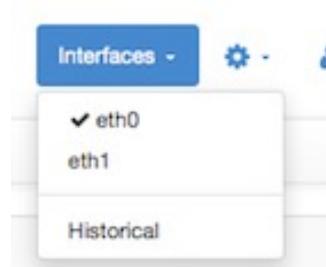


Figure 66 - Interfaces Menu

In addition to physical interface user can also specify a ZMQ endpoint (such as an nprobe instance). The interface page displays as follows:

The screenshot shows the 'Overview' tab for interface 'eth0'. It displays basic information like Id (0), State (Paused), Name (eth0), Family (PF_RING), and Bytes (54.00 MB). A note about overhead bytes is shown. Below this is a 'Traffic Breakdown' section with a pie chart showing packet sizes: Local-Large (77.8%), Local-Small (15.7%), Remote-Small (7.3%), and Remote-Large (0.0%). At the bottom, it shows Ingress Traffic (53.94 MB [364,568 Pkts]), Received Packets, and Dropped Packets.

Figure 67 - Interfaces Default View

In this page (Overview) user can review information about the interface, such as Id, Family and the overall traffic counter (received and dropped) in bytes. It is possible to customize the name of interface in order to give a meaningful name to it by just writing its name into Custom Name field and pressing the "Save Name" button. It is also possible to pause in order to temporarily stop monitoring activity. Other views are:

Packets View: this page describes in a pie chart a packet size distribution.

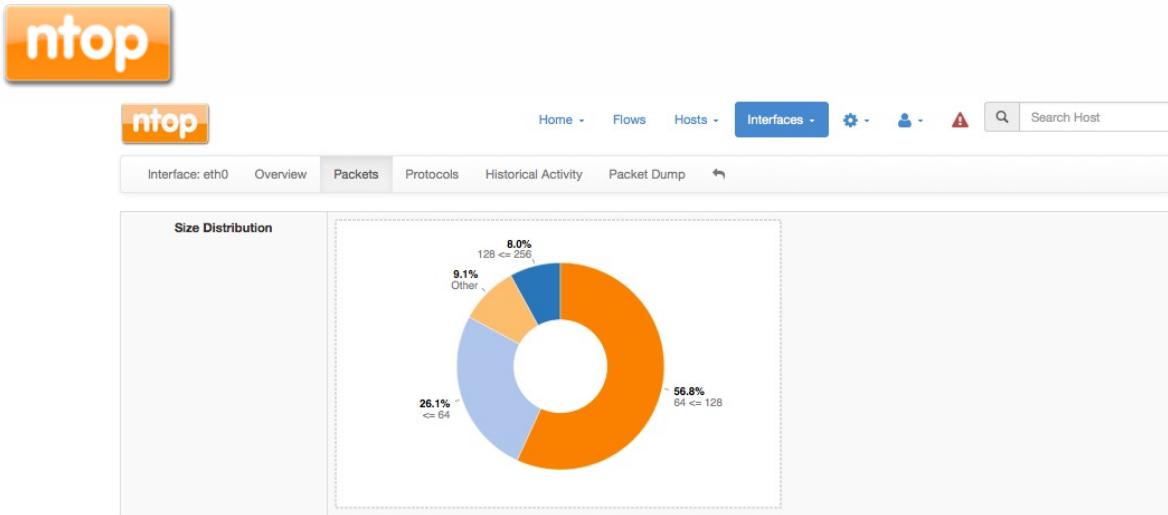


Figure 68 - Interfaces Packets View

Protocol View: this page provides three pie charts and a specific table with the protocol detected on the selected interface.

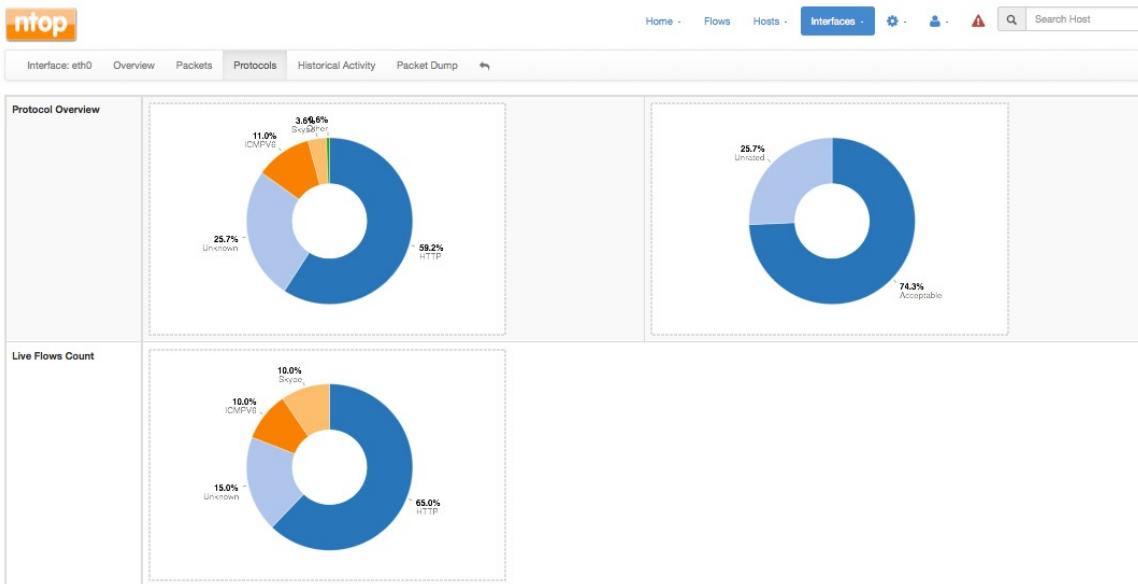


Figure 69 - Interfaces Protocols View

In the two upper pie charts ntopng shows the application distribution and its categorization distribution. The lower pie chart shows the live flows count currently active. All labels of the pie charts are links to relative pages for active flows with that protocol. In these pie charts the page provides a list of protocols detected with total traffic since startup and two types of representation of the percentage, graphic and numeric way as represented below:

Application Protocol	Total (Since Startup)	Percentage
Unknown ⓘ	12.3 MB	21.5 %
Skype ⓘ	1.71 MB	3 %
SSH ⓘ	147.63 KB	0.25 %
MDNS ⓘ	64.63 KB	0.11 %
ICMPv6 ⓘ	5.25 MB	9.19 %
ICMP ⓘ	244 Bytes	0 %
HTTP ⓘ	28.34 MB	49.56 %
DHCP ⓘ	77.39 KB	0.13 %

Figure 70 - Interfaces Protocols Table



By selecting Application Protocol value you can display a Historical Activity page for that protocol (see below) and by clicking magnifying lens icon you can display all active flows for that protocol. For instance if your interest is the Skype protocol you can display the following pages:

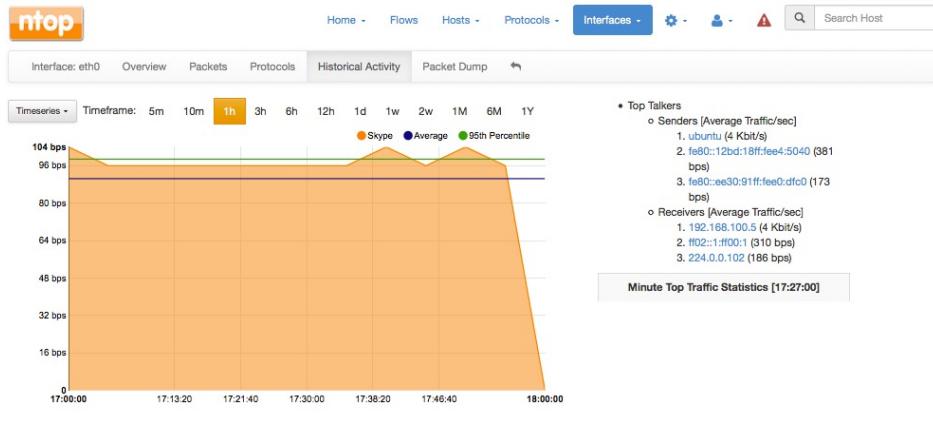


Figure 71 - Interfaces Historical Activity View



Figure 72 - Active Flows

In this page if you select Application value (in this case Skype) you can display all hosts using that protocol.

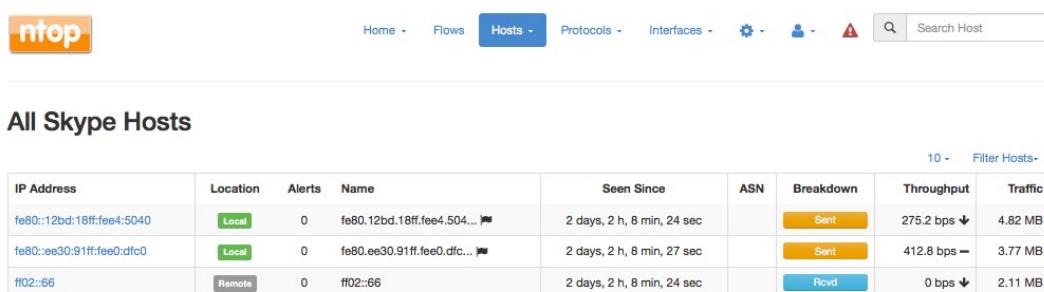


Figure 73 - Application Hosts Table

Historical Activity: this page provides a historical view of the traffic on interface.

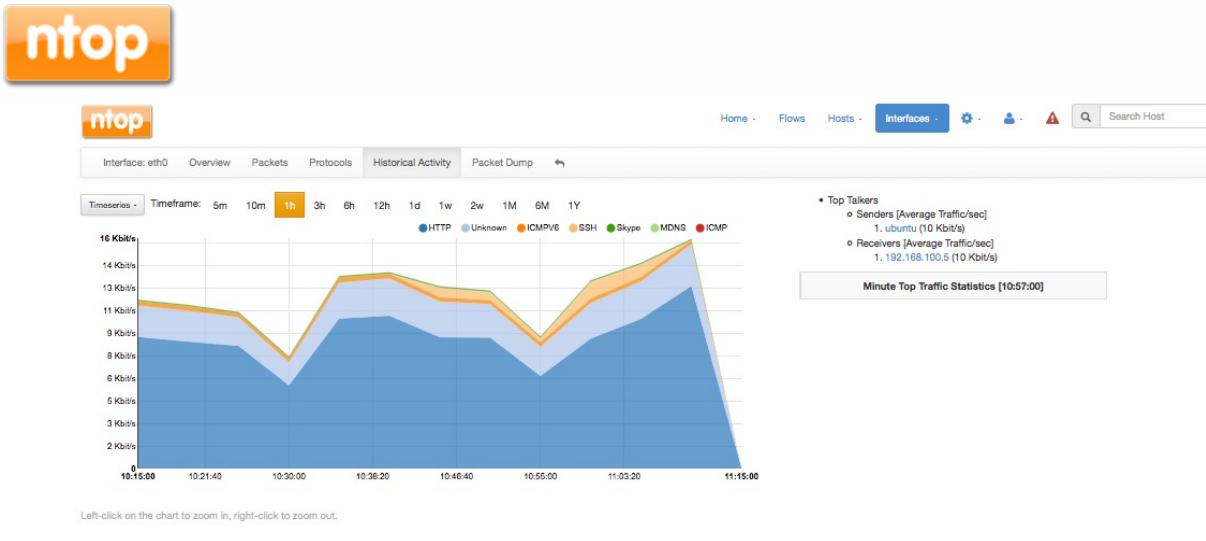


Figure 74 - Intefaces historical global view

(all protocols graph)



Figure 75 - Interfaces Historical Filtered View

(all traffic graphs)

The Time series can be adjusted to analyze by selecting Timeframe values from 5 minutes up to 1 year. In the same way it can be selected either all or just one or more protocol, by selecting the button named Time series. The content of the page is shown by a graphic for timeframe selected and a table with summarized statistics information for that period. The image above describes two Timeseries, All Protocols and Total Traffic.

Ntopng is Vlan aware, hence if several Vlans are detected, traffic is accounted also on Vlan basis.

Packet Dump: this page sets the possibility to instruct ntopng to handle captured traffic in a specific way and not just analyze it. The all traffic can be saved to disk or just the one marked as unknown bu the nDPI library and, in addition to those, traffic can be also be replicated on a network tap (setup by ntopng on installation/startup) and this allows the user to analyze that traffic in the preferred way (i.e.: starting a wireshark session on the network tap).

Figure 76 - Interfaces Packet Dump View

• Other Menus

We have a graphical menu which list Settings, Administration, Alerts (if necessary) and Search Host.



Figure 77 - Other Menus

Setting Menu



Figure 78 - Gear Icon

The Gear icon opens the Setting Menu where 3 items are available:

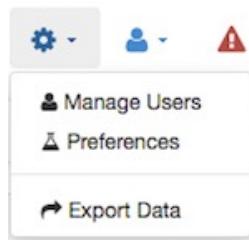


Figure 79 - Setting Menu

Manage Users: this menu item allows to manage ntopng users.

Ntopng (if started with the authentication active) is a multiuser system and several simultaneous users can be active. Users can be either Administrators or standard users. (user role dropdown)

Username	Full Name	Group	Edit
admin	ntopng Administrator	administrator	Manage

Showing 1 to 1 of 1 rows

Figure 80 - Users Table

For each user you can edit some information by selecting the *manage* button, where password and some preferences such as role and allowed networks can be changed in this popup menu:

New User Password

Confirm New User Password

Change User Password

User Role

Allowed Networks

Comma separated list of networks this user can view. Example: 192.168.1.0/24,172.16.0.0/16

Change User Preferences

Close

Figure 81 - Edit User Preference

Administrators cannot change configuration but they can modify some parameters. Preferences this menu permits to change some runtime configuration:

Figure 82 - Runtime Preferences

Report Visualization

Throughput Unit

To select the throughput unit to be displayed in traffic reports: bytes or packets;

Traffic Storage (RRD): this menu item refers to RRD databases creation for local hosts and/or for each nDPI protocol detected.

RRDs For Local Hosts

Toggle the creation of RRDs for local hosts. Turn it off to save storage space: on/off.

nDPI RRDs For Local Hosts

Toggle the creation of nDPI RRDs for local hosts. Enabling their creation allows you to keep application protocol statistics at the cost of using more disk space: on/off

Alerts: this menu permits to set thresholds to alert on specific conditions. In this case ntopng is able to evaluate them and advise the user issuing an alert. ntopng is able to report alerts to system syslog (allowing users to create rules to handle these alerts in specific manner).

Alerts On Syslog

Toggle the dump of alerts on syslog: on/off.

Host Flow Alert Threshold

Max number of new flows/sec over which a host is considered a flooder. Default: 25.

Host SYN Alert Threshold

Max number of TCP SYN packets/sec over which a host is considered a flooder. Default: 10.

Nagios Configuration: ntopng has embedded the capability to act as a remote Nagios probe, hence here user can set the required parameters.

Alerts On Nagios

Toggle sending events to Nagios.

Nagios Daemon Host

Address of the host where the Nagios daemon is running. Default: localhost.

Nagios Daemon Port



Port where the Nagios daemon is listening. Default: 5667.

Nagios Terminal Configuration

Configuration used by the send_nsca utility to send events to the Nagios daemon. Default: /etc/nagios/send_nsca.cfg.

Data Purge: this menu item permits to change the memory footprint of ntopng changing the way it should be freed from inactive objects.

Local Host Idle Timeout

Inactivity timeout after a local host is considered idle (sec). Default: 300.

Remote Host Idle Timeout

Inactivity timeout after a remote host is considered idle (sec). Default: 60.

Flow Idle Timeout

Inactivity timeout after a flow is considered idle (sec). Default: 60.

Virtual HTTP Server Traffic

Save HTTP Server Traffic

Toggle dumping on disk virtual HTTP server traffic. Turn it off to save storage space.

Export Data: ntopng is able to export host's monitoring information.

It allows to export ntopng data in JSON format giving the user the ability to include ntopng information in a user created GUI.

Export Data

Host
 IP or MAC Address

NOTE: If the field is empty all hosts will be exported

Vlan:
 Vlan

NOTE: If the field is empty vlan is set to 0.

Figure 83 - Export Data Page

Administration Menu



Figure 84 - User Icon

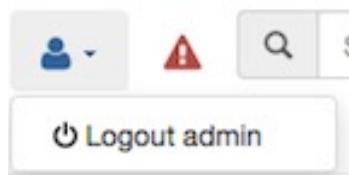


Figure 85 - User Menu

This menu contains logout item to disconnect ntopng GUI.



Alerts Menu



Figure 86 - Alert Icon

The Alerts Menu provides the issued alerts triggered based on settings specified either in the Preferences menu (overall alerts) and each specific host thresholds. This icon is hidden if no alerts are triggered or after purge operation by GUI user. The Alerts Menu shows a page as below:

The screenshot shows the 'Queued Alerts' section of the nTop interface. At the top, there are navigation links: Home, Flows, Hosts, Protocols, Interfaces, and a search bar labeled 'Search Host'. Below the navigation is a red alert icon. The main area displays a table of alerts with columns: Action, Date, Severity, Type, and Description. The table lists 64 rows of alerts, all of which are 'Error' level TCP SYN Flood events from host 192.168.100.5. The last row shows a timestamp of Tue Apr 28 17:47:23 2015.

Action	Date	Severity	Type	Description
[Icon]	Tue Apr 28 17:51:33 2015	Error	▲ TCP SYN Flood	Host 192.168.100.5 is under SYN flood attack [3786 SYNs received in the last 3 sec] TCP 192.168.100.1:42074 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:51:33 2015	Error	▲ TCP SYN Flood	Host 192.168.100.1 is a SYN flooder [3786 SYNs sent in the last 3 sec] TCP 192.168.100.1:42074 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:50:32 2015	Error	▲ TCP SYN Flood	Host 192.168.100.5 is under SYN flood attack [3412 SYNs received in the last 3 sec] TCP 192.168.100.1:41698 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:50:32 2015	Error	▲ TCP SYN Flood	Host 192.168.100.1 is a SYN flooder [3412 SYNs sent in the last 3 sec] TCP 192.168.100.1:41698 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:49:29 2015	Error	▲ TCP SYN Flood	Host 192.168.100.5 is under SYN flood attack [3034 SYNs received in the last 3 sec] TCP 192.168.100.1:41320 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:49:29 2015	Error	▲ TCP SYN Flood	Host 192.168.100.1 is a SYN flooder [3034 SYNs sent in the last 3 sec] TCP 192.168.100.1:41320 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:48:26 2015	Error	▲ TCP SYN Flood	Host 192.168.100.5 is under SYN flood attack [2656 SYNs received in the last 3 sec] TCP 192.168.100.1:40942 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:48:26 2015	Error	▲ TCP SYN Flood	Host 192.168.100.1 is a SYN flooder [2656 SYNs sent in the last 3 sec] TCP 192.168.100.1:40942 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:47:23 2015	Error	▲ TCP SYN Flood	Host 192.168.100.5 is under SYN flood attack [2278 SYNs received in the last 3 sec] TCP 192.168.100.1:40564 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]
[Icon]	Tue Apr 28 17:47:23 2015	Error	▲ TCP SYN Flood	Host 192.168.100.1 is a SYN flooder [2278 SYNs sent in the last 3 sec] TCP 192.168.100.1:40564 > 192.168.100.5:3000 [proto: 0/Unknown][1/0 pkts][74/0 bytes]

Showing 1 to 10 of 64 rows

[Navigation icons: back, forward, first, last, page numbers 1-5]

[Purge All Alerts](#)

Figure 87 - Alert Page

Each row describes an alert detected by ntopng with information such as Date, Severity, Type and Description. In the case shown above we have a host that attempted a lot of connections to other hosts. This means that this host generates a number of flows greater than threshold value established. We can purge all alerts one time or individually.

Search Host

Figure 88 - Search Bar

This window permits to display all information about a specific host. Dynamic auto completion allows users to check whether the searched host appears in the list while typing. Selecting the host, ntopng jump to host info page.



Additional ntopng Features

ntopng is able to do much more than this including:

- Ability to work in inline mode and enforce traffic and layer-7 protocols
- Integrate with external applications such as Nagios for alerting and be used as source of monitoring data
- Embedded-Systems aware including Raspberry Pi and Ubiquity Networks.
- SNMP support

Please follow the ntop blog (<http://blog.ntop.org>) for all the latest news.