



ntopng User's Guide

Version 2.0

November 2015



Index

Preface	4
What is ntopng?	4
How to start ntopng?	4
How ntopng works.	9
Home Menu	11
About ntopng	11
ntop Blog.....	12
Report an Issue	12
Dashboard.....	12
Dashboard	13
Dashboard in the Community Version	13
Dashboard in the Professional Version	18
Report.....	19
Flows.....	22
Application	22
Layer-4 Protocol (L4 Proto)	23
Client	23
Server	23
Duration.....	23
Breakdown	23
Actual Throughput.....	23
Total Bytes.....	23
Info	23
Hosts.....	25
All Hosts	25
Networks	26
Autonomous Systems.....	26
Countries.....	27
Operating Systems.....	27
HTTP Servers (Local).....	27
Top Hosts (Local).....	28
Geo Map	28
Tree Map	29
Local Flow Matrix	29
Host Details	30
Home	30
Traffic.....	31
Packets	32
Ports.....	33
Peers	34
Protocols	35
DNS.....	36
HTTP	37
Flows	38
SMNP	38
Talkers	39
Geography	39

Similarity.....	39
Alerts Configuration	40
Statistics	41
Interfaces.....	42
Home	43
Packets	43
Protocols	44
Statistics	45
Traffic Profiles (Professional Version)	46
Packet Dump	46
• Other Menus	47
Setting Menu	47
Administration Menu	50
Alerts Menu	51
Search Host.....	51
Additional ntopng Features.....	52



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-dir -d] <path>	Data directory (must be writable).
	Default: /var/tmp/ntopng
[--daemon -e]	Daemonize ntopng
[--httpdocs-dir -1] <path>	HTTP documents root directory.
	Default: httpdocs
[--scripts-dir -2] <path>	Scripts directory.
	Default: scripts
[--callbacks-dir -3] <path>	Callbacks directory.
	Default: scripts/callbacks
[--no-promisc -u]	Don't set the interface in promiscuous mode.
[--categorization-key -c] <key>	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).



```
[--http-port|-w] <[:.]http port>
[--https-port|-W] <[:.]https port>
[--local-networks|-m] <local nets>
[--ndpi-protocols|-p] <file>.protos
[--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-num-hosts|-x] <num>
[--users-file|-u] <path>
[--pid|-G] <path>
[--disable-alerts|-H]
[--packet-filter|-B] <filter>
[--dump-flows|-F] <mode>
[--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]
[--help|-h]

| Please read README.httpb1 for
| more info.
| HTTP port. Set to 0 to disable http server.
| Prepend a : before the port to listen to the
| loopback address. Default: 3000
| HTTPS port. See usage of -w above. Default: 3001
| Local nets list (default: 192.168.1.0/24)
| (e.g. -m "192.168.0.0/24,172.16.0.0/16")
| Specify a nDPI protocol file
| (eg. protos.txt)
| Disable host persistency in the Redis cache
| Redis host[:port] [@database id]
| Run ntopng with the specified user
| instead of nobody
| Do not change user (debug only)
| Terminate when a pcap has been read (debug only)
| Disable web interface logout for inactivity
| Disable user login authentication:
| 0 - Disable login only for localhost
| 1 - Disable login only for all hosts
| Max number of active flows
| (default: 131072)
| Max number of active hosts
| (default: 65536)
| Users configuration file path
| Default: ntopng-users.conf
| Pid file path
| 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
|     Don't flush hosts (default: none).
|   Values:
|     all    - Keep all hosts in memory
|     local  - Keep only local hosts
|     remote - Keep 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
|   Print version and quit
|   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.

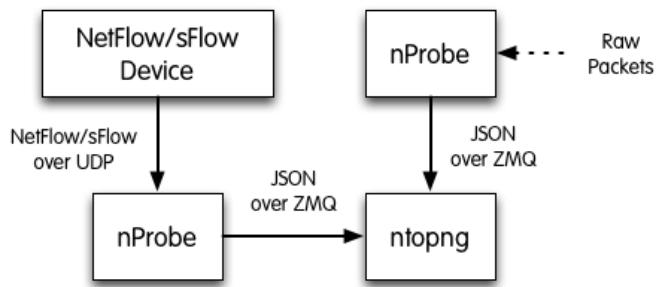


Figure 1 - ntopng/nprobe setup

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.





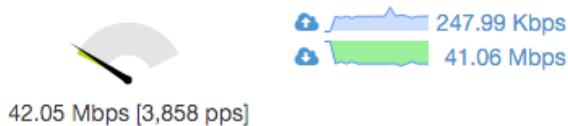
The items list are *Home*, *Flows*, *Hosts*, *Protocols*, *Interfaces*, *Setting*, *Logout*, and *Search Host*. An extra item *Alert* pops out when some alerts fired in reaction of user configuration.

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.

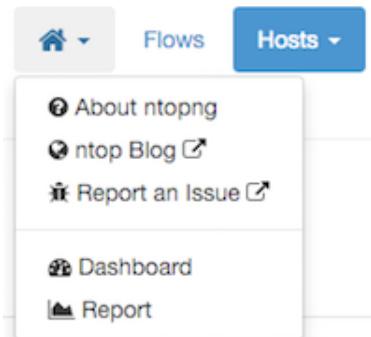
Uptime: 51 min, 30 sec
 2 Alerts 49 Hosts 49 Flows

The Right Side of the Footer Bar

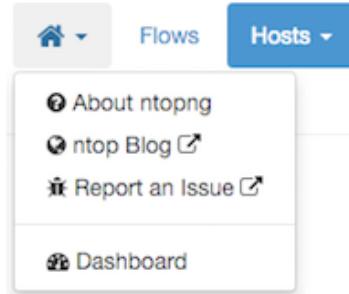


Home Menu

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	24FCFFE14BF4ADEF272527550C591E9311460564450CC [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.

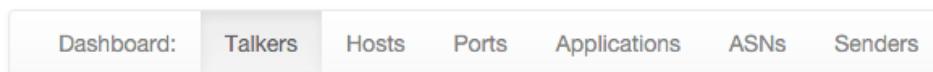


Dashboard

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

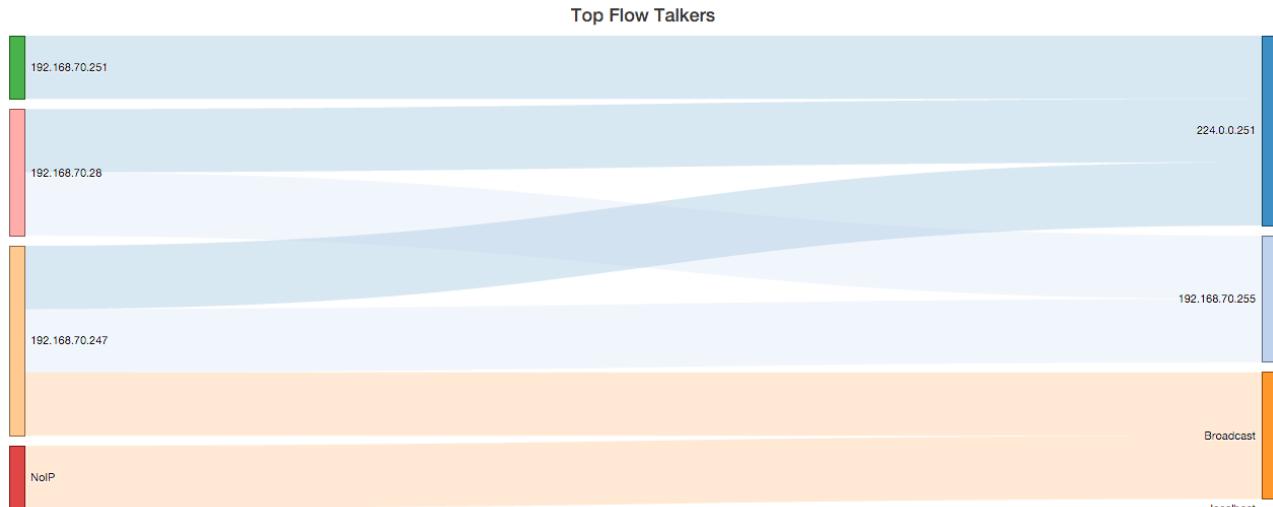
The dashboard provides information about Talkers, Hosts, Ports, Applications, ASNs, and Senders. Information can be selected from the top menu. Each item is discussed below.



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: 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.

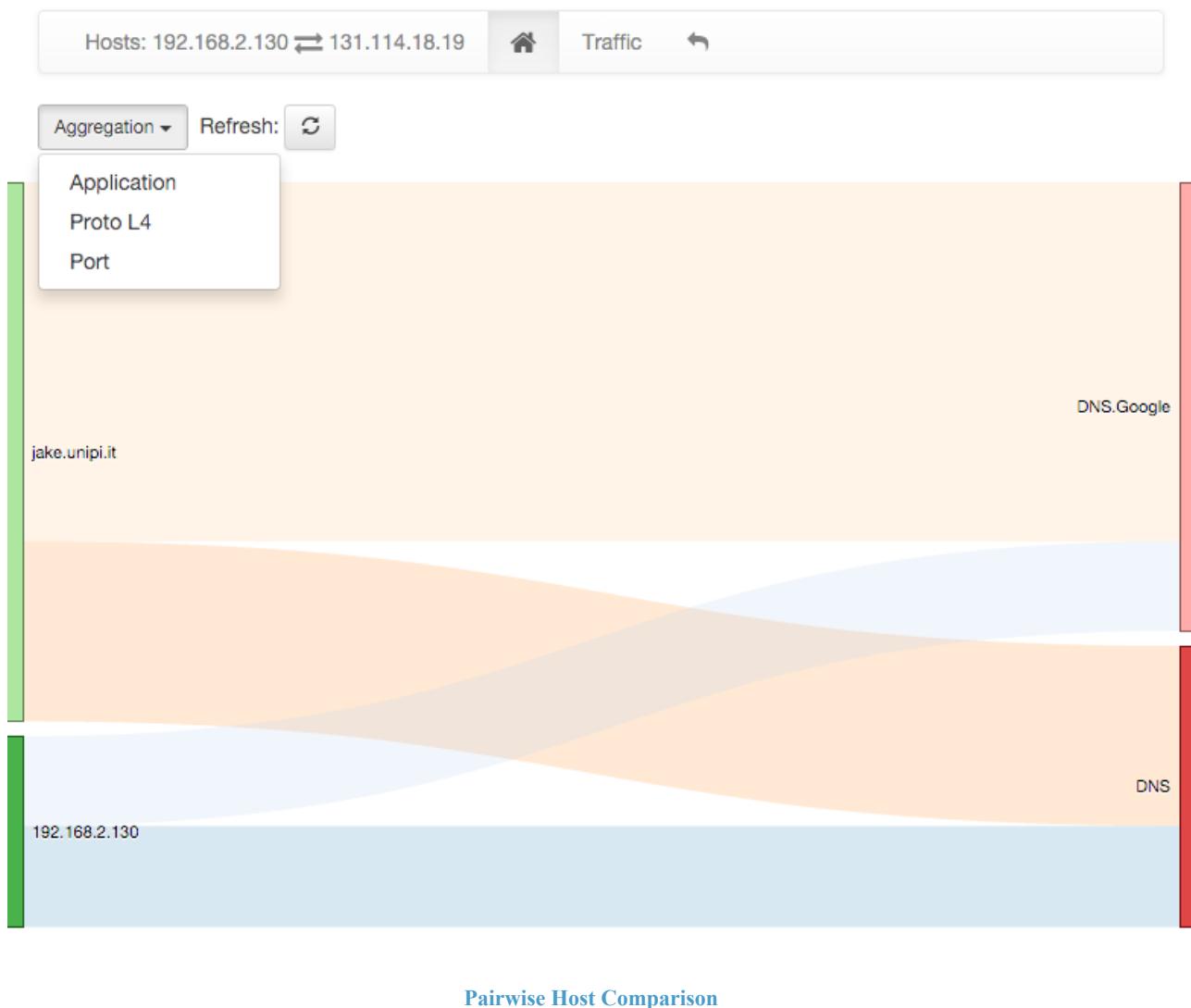


Host and flow information shown in the Sankey is interactive. Indeed, both host names (IP addresses) as well as flows are clickable.

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.



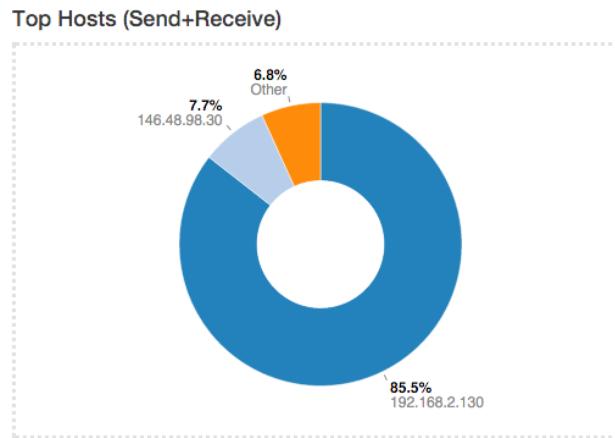
Pairwise Host Comparison



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.

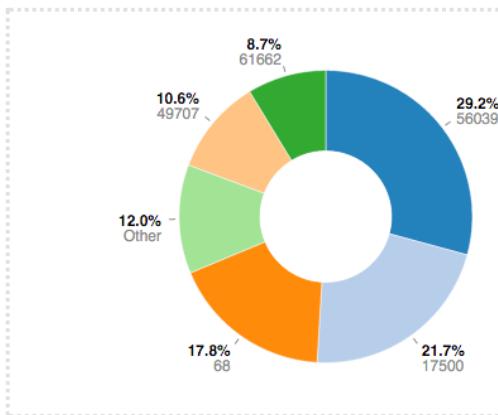


Pie Chart of Top Hosts

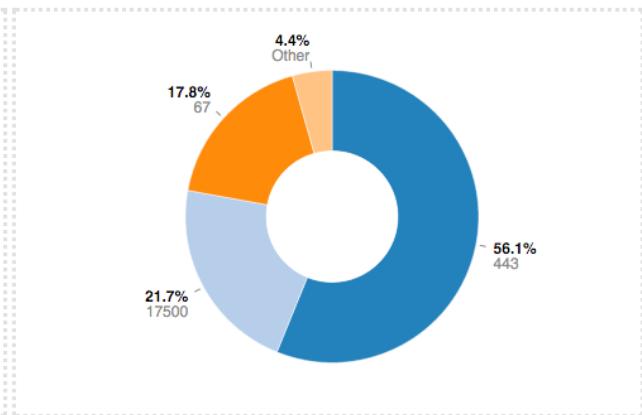
Ports

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

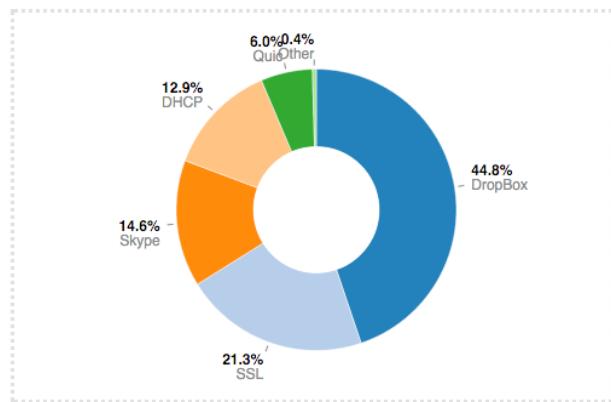
Any port number shown can be double-clicked to visit the ‘Active Flows’ page. This page lists all the currently active flows such that client or server port matches the one clicked.



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



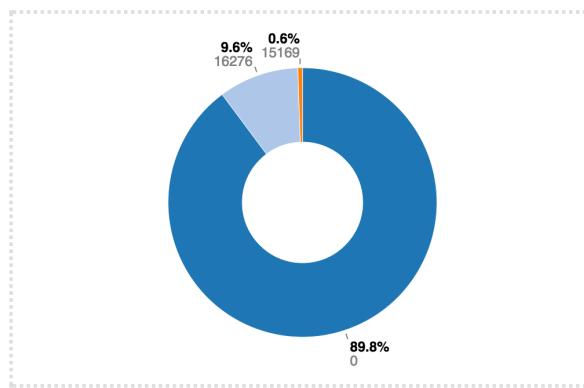
Pie Chart of Top Applications

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



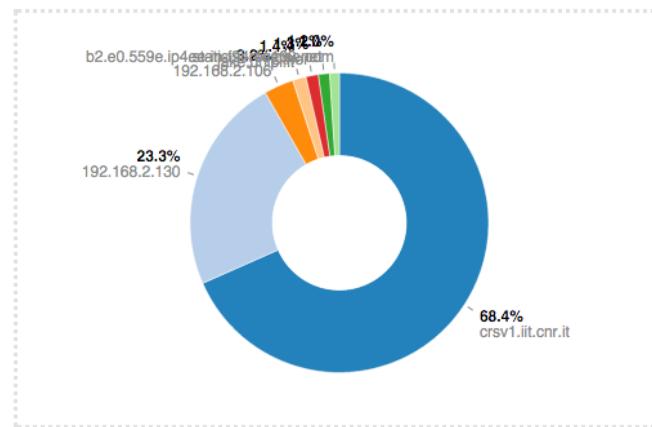
Pie Chart of Top ASNs



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



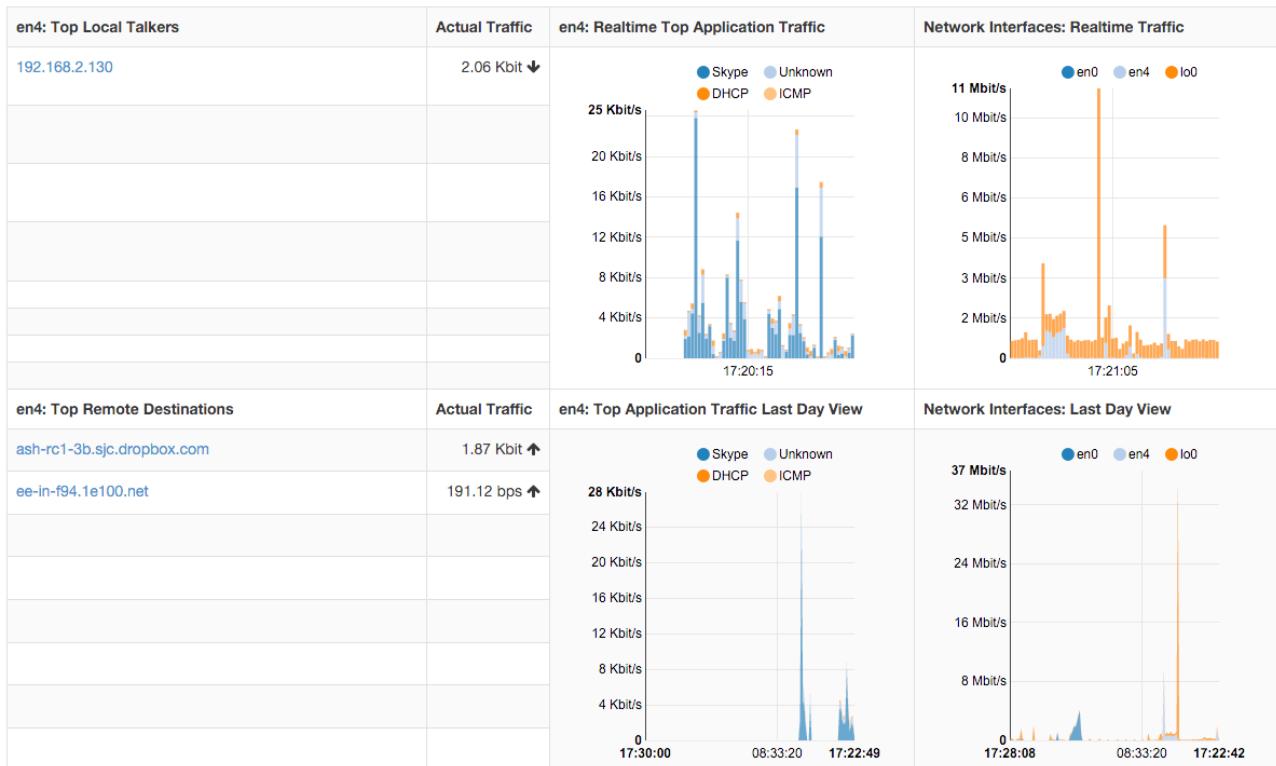
Pie Chart of Top

The Dashboard in the Professional Version



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 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 allows to generate custom traffic reports for one or more interfaces monitored. Report page, reachable from the dropdown home menu in the main toolbar, presents the user with multiple configuration options

The Top of the Report Page

Fixed-width temporal intervals are available on the left. They are 1h (one hour), 1d (one day), 1w (one week), 1M (one month), 6M (six months), and 1Y (one year). A click on any of those intervals produces an automatic report that spans a time range that starts at the present and that goes backwards in time until the clicked interval is reached.

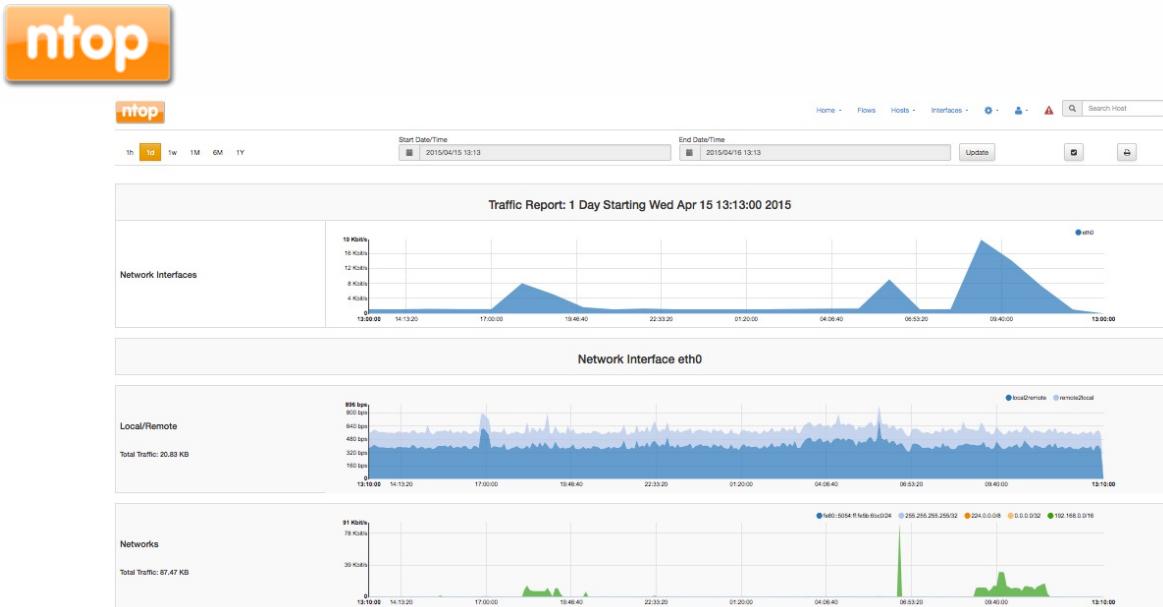
Exact temporal intervals can be chosen using the two dropdown date time pickers in the center. The first and the second pickers are used to specify the start and the end of a custom report, respectively. Once dates and times have been chosen, the report is obtained by clicking on 'Generate'.

The small checkbox icon right of the 'Generate' button allows to select one or more of the available monitored interfaces, as well as application protocols of interest. Clicking on it yields the following overlaid menu

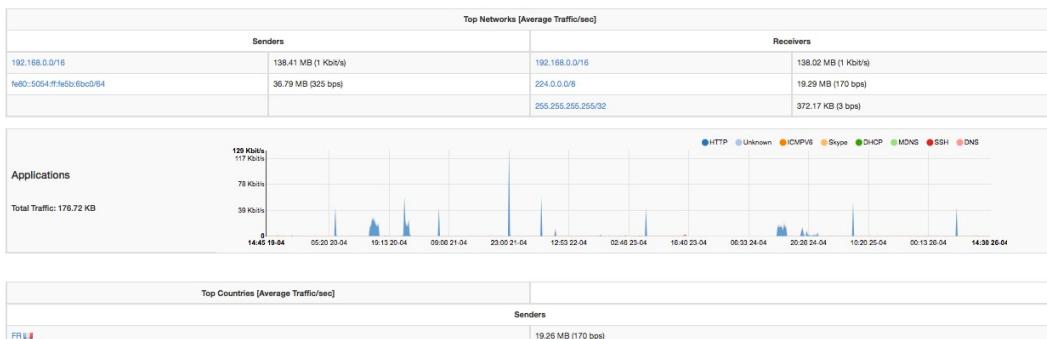
Network Interfaces	Protocols
<input type="checkbox"/> Toggle All	<input type="checkbox"/> Toggle All
<input type="checkbox"/> view:en0,en4,lo0	<input type="checkbox"/> Apple
<input type="checkbox"/> lo0	<input type="checkbox"/> AppleCloud
<input type="checkbox"/> en4	<input type="checkbox"/> AppleiTunes
<input checked="" type="checkbox"/> en0	<input type="checkbox"/> DNS
	<input type="checkbox"/> DropBox
	<input type="checkbox"/> GMail
	<input type="checkbox"/> Google
	<input type="checkbox"/> HTTP
	<input type="checkbox"/> IGMP

Report Filter Overlay

Finally, the rightmost icon generates a printer-friendly report ready to be printed or exported to PDF.



Generated Report - Network Interfaces and Traffic

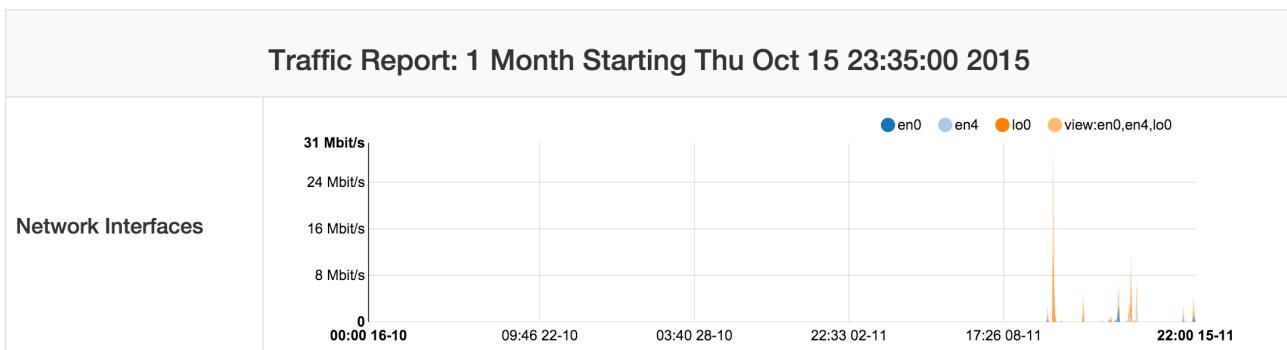


Generated Report - Top Networks and Applications

Reports contain charts of monitored interfaces overall traffic, local versus remote traffic, local networks traffic, as well as the traffic grouped by:

- Application Protocols (e.g., HTTPS, Skype)
- Countries
- Local Hosts (hosts belonging to local networks) and Remote Hosts (hosts belonging to remote networks)
- Local Operating Systems
- Autonomous Systems

In the remainder of this section are screenshots of reported information discussed above.



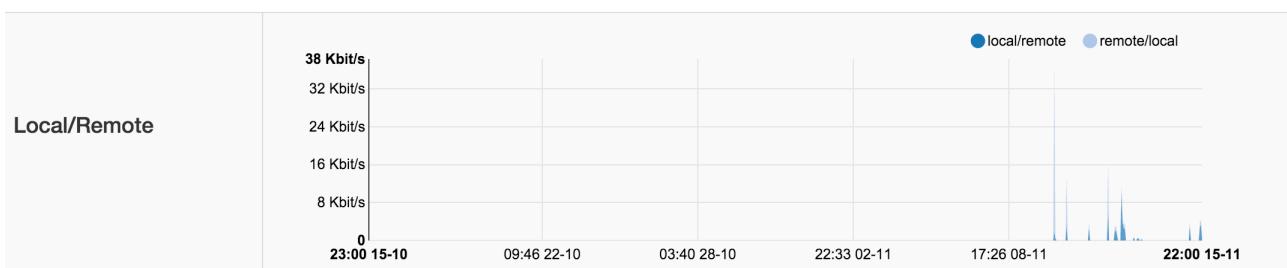
Report - Monitored Network Interfaces Summary



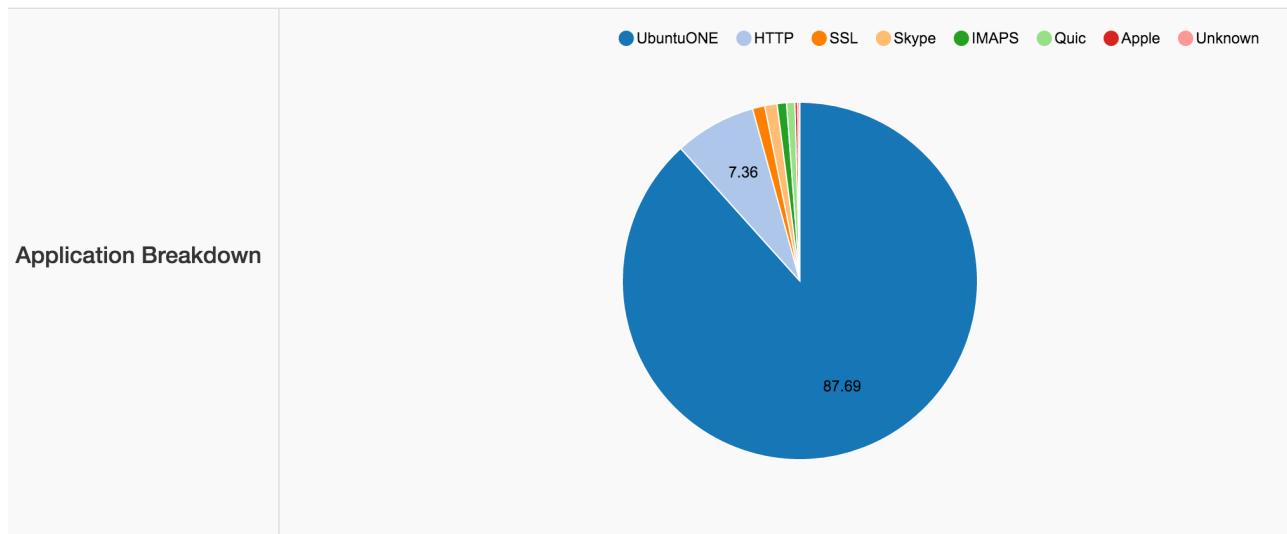
Top Networks [Average Traffic/sec]

Senders		Receivers	
192.168.2.0/24	14.40 MB (45 bps)	192.168.2.0/24	1.25 GB (4 Kbit/s)
146.48.98.0/24	1.09 MB (3 bps)	146.48.98.0/24	416.23 KB (1 bps)
8.8.8.0/24	1.42 KB (< 1 bps)	8.8.8.0/24	1.12 KB (< 1 bps)

Report - Top Local Networks



Report - Local to Remote and Remote to Local Traffic



Report - Application Breakdown

Top Countries [Average Traffic/sec]			
Senders		Receivers	
GB 🇬🇧	1.15 GB (4 Kbit/s)	GB 🇬🇧	10.65 MB (33 bps)
IT 🇮🇹	102.30 MB (320 bps)	IT 🇮🇹	1.61 MB (5 bps)
US 🇺🇸	5.60 MB (18 bps)	US 🇺🇸	1.03 MB (3 bps)

Report - Top Countries



Flows

The ‘Flows’ entry in the top toolbar can be selected to visualize realtime traffic information on the currently active flows. A flow can be thought of as a logical, bi-directional communication channel between two hosts¹. Multiple simultaneous flows can exist between the same pair of hosts.

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
info	HTTP	TCP	192.168.2.130:52303	mirror2.mirror.garr.... :http	36 sec	Server	41.19 Mbit	172.38 MB	/mirrors/ubuntu-releases...
info	Redis	TCP	localhost:65316	localhost:6379	32 min, 13 sec	Client Server	33.74 Kbit	23.68 MB	

[Active Flows Page](#)

Flows are uniquely identified via a 5-tuple composed of:

- Source and destination IP address
- Source and destination port
- Layer-4 protocol

Each flow is shown as a row entry in the flows table. Flows are sortable by application using the rightmost dropdown menu at the top right edge of the table. Similarly, the other dropdown menu enables the user to choose the number of flows displayed on each page.

Flows have multiple information fields, namely, Application, Layer-4 Protocol, Client and Server hosts, Duration, Client and Server Breakdown, Current Throughput, Total Bytes, and Additional Information. Information fields are briefly discussed below.

Application

Application is the Layer-7 program which is exchanging data through the flow. This is the piece of software that lays closest to the end user. Examples of Applications are Skype, Redis, HTTP, and Bit Torrent. Layer-7 applications are detected by the NTOPIP open source Deep Packet Inspection (DPI) engine named nDPI². In case application detection fails, ntopng marks the flow as ‘Unknown’. If the detection succeeds, the application name and a thumb up (down) is shown if the application is deemed to be good (bad).

Application name can be clicked to see all hosts generating traffic for the application.

¹ Actually, flows may also exist between a host and a multicast group, as well as a broadcast domain.

² <https://github.com/ntop/nDPI>



Layer-4 Protocol (L4 Proto)

The layer-4 protocol is the one used at the transport level. Most common transport protocol are the reliable Transmission Control Protocol (TCP) and the best-effort User Datagram Protocol (UDP).

Client

This field contains host and port information regarding the client endpoint of the flow. A host is considered a client if it is the initiator of the flow. Information is shown as host:port and both information are clickable. If the host has a public IP address, ntopng also shows the country flag for that client³. A blue flag is drawn when the host is the ntopng host.

Server

Similarly to the client, this field contains information regarding the server endpoint of the flow. A host is considered a server if it is not the initiator of the flow. We refer the reader to the previous paragraph for a detailed description.

Duration

This is the amount of time that has elapsed since the flow was opened by the client.

Breakdown

Flows are bi-directional, in the sense that traffic flows both from the server to the client and from the client to the server. This colored bar gives an indication on the amount of traffic exchanged in each of the two directions. Client to server traffic is shown in orange, while server to client in blue.

Actual Throughput

TODO: how is throughput defined and implemented?

Total Bytes

The amount of traffic exchanged through the flow. This total value is the sum of traffic exchanged in each of the two directions (client to server and server to client).

Info

Extra information nDPI is able to extract from the detected flow is made available in this field. This field may include urls, traffic profiles (in the Professional Version), contents of DNS requests, and so on.

³ These data are based on MaxMind databases.



The leftmost column *Info* has a button that redirects the user to a page containing detailed flow information. Values in the Flow Details page are dynamically updated every second. Detailed information include

- First / Last Seen
- Total Traffic Volume and Trend⁴
- Client / Server Traffic Breakdown
- Packets and Bytes sent in each flow direction
- Protocol flags, if L4 protocol is TCP
- SSL Certificate
- Throughput
- Flow traffic dump to persistent storage.

Flow: 192.168.1.92:54949 ⇢ 93-62-150-157.ip23.fastwebnet.it:443		Overview	◀
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			

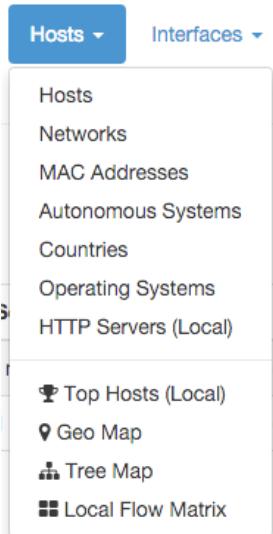
[Flow Details Page](#)

⁴ Increasing trend is shown with an arrow that points upwards. Stable trend is shown with a dash. Decreasing trend is show with as arrow that points downwards.



Hosts

Hosts is a dropdown menu always reachable from the top toolbar that contains a bunch of links to host-related information pages. The dropdown is as follows



The Hosts Dropdown Menu

Host-related information pages available have the following content

- *Hosts* page shows all hosts seen
- *Networks* page lists all networks — both local and remote — any seen host belongs to
- *MAC Addresses* page has the list of Level-2 Addresses for the hosts seen
- *Autonomous Systems* page presents all Autonomous Systems (AS) any seen host belongs to
- *Countries* page shows hosts countries based on the information provided by MaxMind databases
- *Operating Systems* page lists all host operating systems that have been detected. Detection is done using passive fingerprinting techniques
- *HTTP Servers (Local)* page shows monitored HTTP servers, limited to local hosts only
- *Top Hosts Traffic* page presents traffic of top hosts in order to typology selected;
- *Geo Map* page lays out hosts in a geographic map to give visual insights into the geographical locations of seen hosts
- *Tree Map* page shows a tree representation of the monitored environment
- *Local Matrix* page displays a matrix representation of local systems

All Hosts

All hosts that have been seen monitoring network interfaces are show here. Column headers can be clicked to sort results in descending (ascending) order of the clicked header. Additional sort options are available in the top right corner of the table.

The table shown has several columns, including

- *IP address*, with optional country flag and OS logo (if detected)
- *Location*, either Local (the host belongs to a local network) or Remote (the host belongs to a remote network) — please note that this is not a geographical location
- *Alerts*, with the number of alerts associated to the host
- *Name*, having the resolved hostname (or a custom name, if set in any Host Details page)



- *Seen Since*, with the amount of time it has lapsed since the first packet sent/received by the host has been observed
- *ASN*, with the AS number (if available)
- *Breakdown*, showing a bar that gives visual insights in the use of both traffic directions
- *Throughput*, with the overall actual throughput of the host
- *Traffic*, with the total traffic exchanged by the host

All Hosts

IP Address	Location	Alerts	Name	Seen Since	ASN	Breakdown	Throughput	Traffic
::1	Remote	0	localhostV6	7 min, 6 sec		Sent Rcvd	220.44 Kbit	432.36 MB
109.73.81.23	Remote	0	ubuntu.ictvalleumbra.it	7 min, 5 sec	ICT Valle Umbra s.r.l.	Sent	277.31 Kbit	14.74 MB
127.0.0.1	Local	0	localhost	7 min, 6 sec		Sent Rcvd	102.17 Kbit	7.5 GB
146.48.98.30	Local	0	crsv1.iit.cnr.it	7 min, 5 sec	Consortium GARR	Sent Rcv	0 bps	3.96 MB
192.168.2.130	Local	0	192.168.2.130	6 min, 54 sec		Sent	0 bps	261.89 KB

[The All Hosts Page](#)

Any host can be clicked to be redirected to its ‘Host Details’ page, which is discussed below.

Networks

Networks shows all networks discovered by ntopng.

Networks

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

[The Networks Summary Page](#)

For each network discovered ntopng provides the number of hosts, alerts triggered, date of discovery, breakdown, throughput and traffic. Network names can be clicked to display the hosts lists inside the network selected.

Autonomous Systems

Autonomous Systems shows all autonomous systems discovered by ntopng.



Autonomous Systems

10 -

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	5 days, 2 h, 3 min, 51 sec	Sent	96 bps ↑	9.84 MB

Showing 1 to 2 of 2 rows

Ntopng uses a Maxmind database to gather information about Autonomous Systems (AS) and based on this it groups hosts belonging to the same AS. AS number 0 contains all hosts having private IP addresses.

Countries

Countries page provides all countries discovered by ntopng. Any country can be clicked to be redirected to a page containing the full list of hosts localized in that country.

Hosts by Country

20 -

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

Showing 1 to 2 of 2 rows

[The Hosts Countries Summary Page](#)

Operating Systems

Operating Systems page shows a list of all OS detected by ntopng. OSes can be clicked to see the detailed list of hosts.

Hosts by Operating System

20 -

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

[The Hosts Operating Systems Summary Page](#)

HTTP Servers (Local)

HTTP Servers page lists all local HTTP Servers. Multiple distinct virtual hosts may refer to the same HTTP server IP, which is specified in the second column. Additional information such as bytes sent and received are available for each HTTP virtual host. By clicking on the magnifying lens icon near to the HTTP virtual host, it is possible to display all active flows involving it.



Local HTTP Servers

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

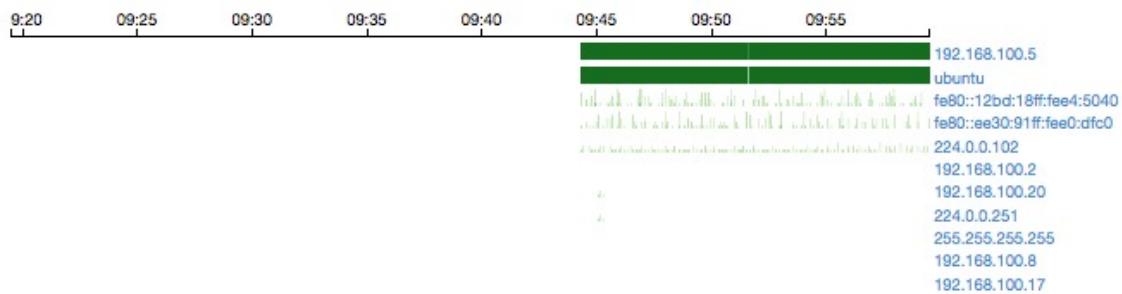
Showing 1 to 1 of 1 rows

[The Local HTTP Servers Summary Page](#)

Top Hosts (Local)

Top hosts page provides hosts activity on time basis. The page should be kept open in order to allow the graph to dynamical update itself with real-time freshly collected data for each host. The time axis is divided in 5-minute bars and goes backwards in time in a right-to-left fashion, starting from the present.

Top Hosts (Local)

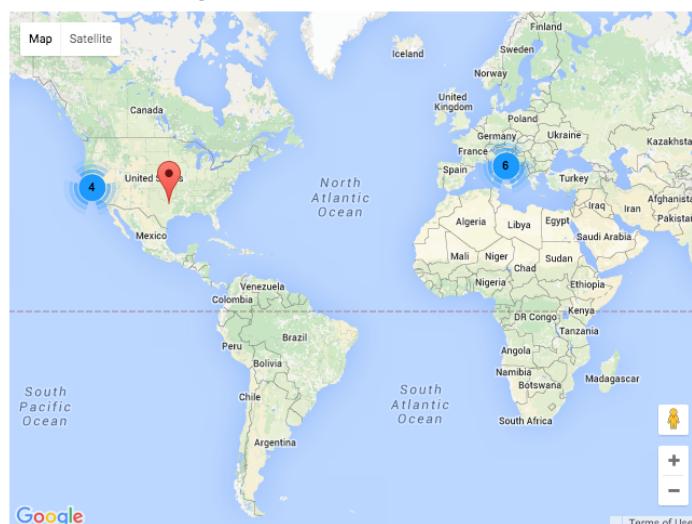


[The Top Hosts Summary Page](#)

Geo Map

The Hosts Geo Map page provides world map where hosts are arranged according to their geographical position.

Hosts GeoMap

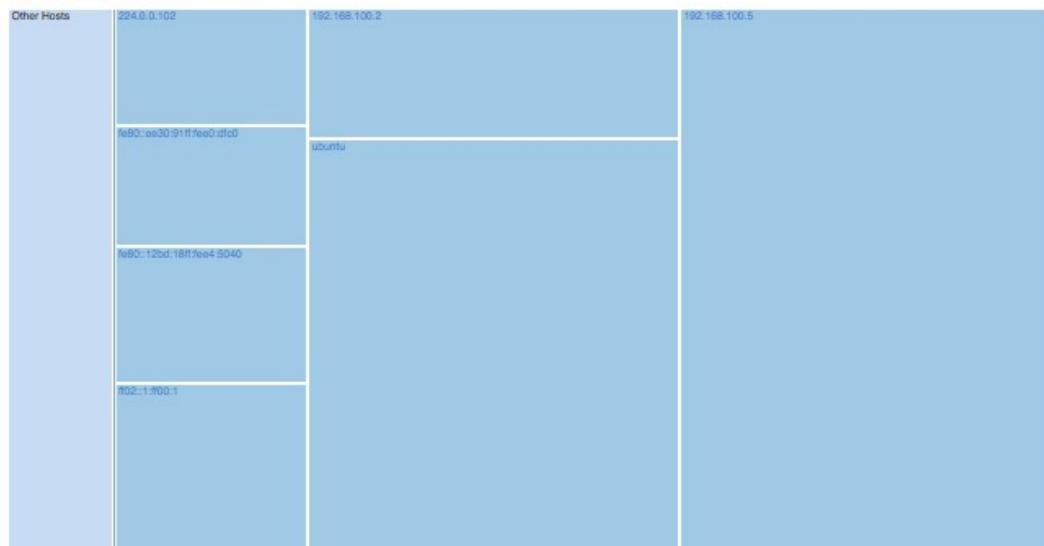


[The Hosts Geo Map Summary Page](#)

Tree Map

This page provides a tree map of all monitored hosts. By clicking on hosts it is possible to visit the corresponding 'Host Details' page.

Hosts TreeMap



[The Hosts Tree Map Summary Page](#)

Local Flow Matrix

Local Hosts Active Flows Matrix page visualizes a matrix of local hosts versus local hosts. Each cell contains the amount of traffic exchanged between every pair of hosts. Since flows are bi-directional, up to two values can be indicated in each cell.

Local Hosts Active Flows Matrix

	192.168.2.255	192.168.2.130	bruno	192.168.2.113	192.168.2.100	crsv1
192.168.2.255		344.63 KB		56.02 KB	66.49 KB	
192.168.2.130	344.63 KB		160 B 80 B			2.45 KB 6.41 KB
bruno		80 B 160 B				
192.168.2.113	56.02 KB					
192.168.2.100	66.49 KB					
crsv1		8.41 KB 2.45 KB				

[The Active Flows Matrix Page](#)



Host Details

Host Details page is as follows.

The screenshot shows the ntop Host Details page for host 192.168.2.130. The top navigation bar includes links for Home, Flows, Hosts (selected), Interfaces, Settings, Users, and Help, along with a search bar. Below the navigation is a toolbar with icons for alert, settings, and graphs. The main content area is divided into sections:

- (Router) MAC Address:** Apple_A7:DE:85 (68:5B:35:A7:DE:85)
- IP Address:** 192.168.2.130 [192.168.2.0/24]
- Name:** 192.168.2.130 (Local) (with "Save Name" button)
- First / Last Seen:** 17/11/2015 09:51:29 [7 min, 34 sec ago] / 17/11/2015 09:58:58 [5 sec ago]
- Sent vs Received Traffic Breakdown:** Sent (yellow bar) and Rcvd (blue bar)
- Traffic Sent / Received:** 1,633,629 Pkts / 2.07 GB — and 698,699 Pkts / 814.17 MB —
- Flows Active / Total:** 'As Client' and 'As Server'
28 — / 304 and 5 — / 20
- TCP Packets Sent Analysis:** Retransmissions (1 Pkts —), Out of Order (13 Pkts —), and Lost (7 Pkts —)
- JSON:** Download link
- Activity Map:** A heatmap showing traffic activity over the last six hours, with a zoom control at the bottom.

The Default View of the Host Details Page

A contextual menu with labels and badges appears right below the top toolbar. Menu entries are dynamic, hence, some of them may not always be present.

Menu entries are discussed below.

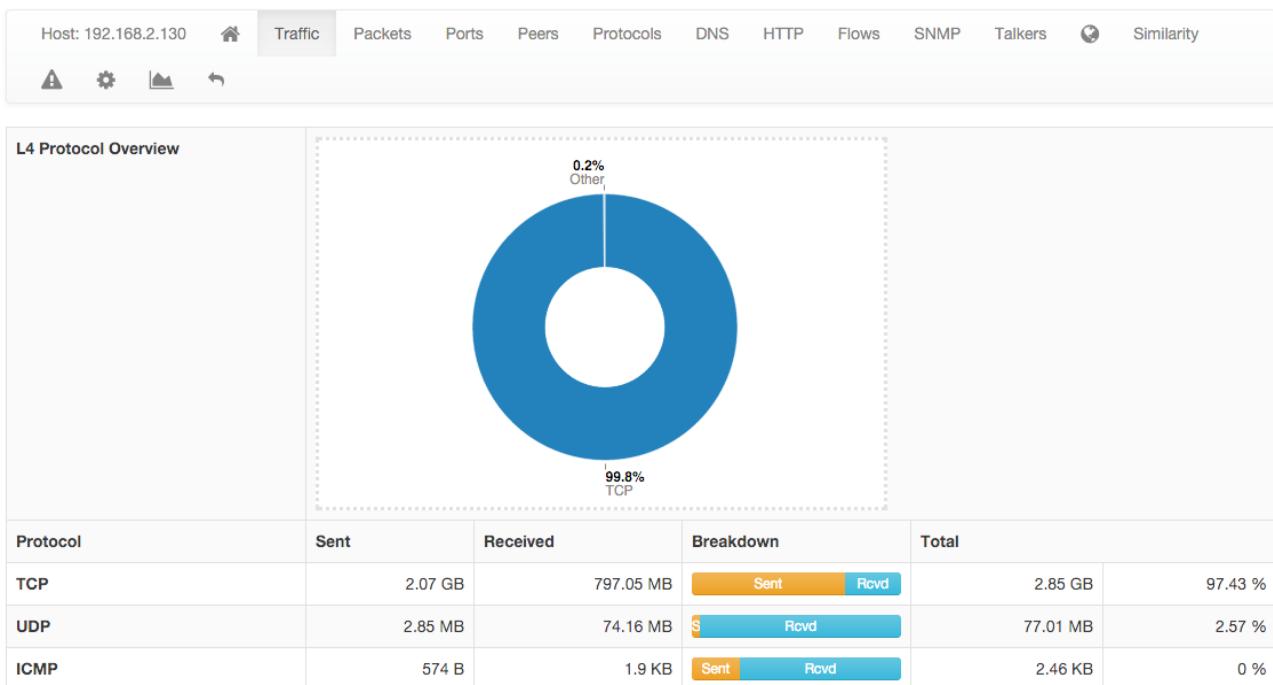
Home

Home is the default view of the Host Details page and provides detailed information including host MAC Address (or the last router MAC address if the host is remote), IP Address (with network mask if detected), a toggle to activate/deactivate alerts for the host, a checkbox to enable packet dump for the specific host, symbolic hostname (or IP address), location (local or remote), 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 'Download' link. The heat map provides the Activity Map for each host. Each box represents one minute of traffic. By default, Activity Map shows the last six hours, but it is possible to set a different timeframe using the controls.



Traffic

The Traffic Page provides Layer-4 protocol statistics for the host. A pie chart showing L-4 protocol breakdown is show at the top of page. A table with detailed statistics is shown below te chart.

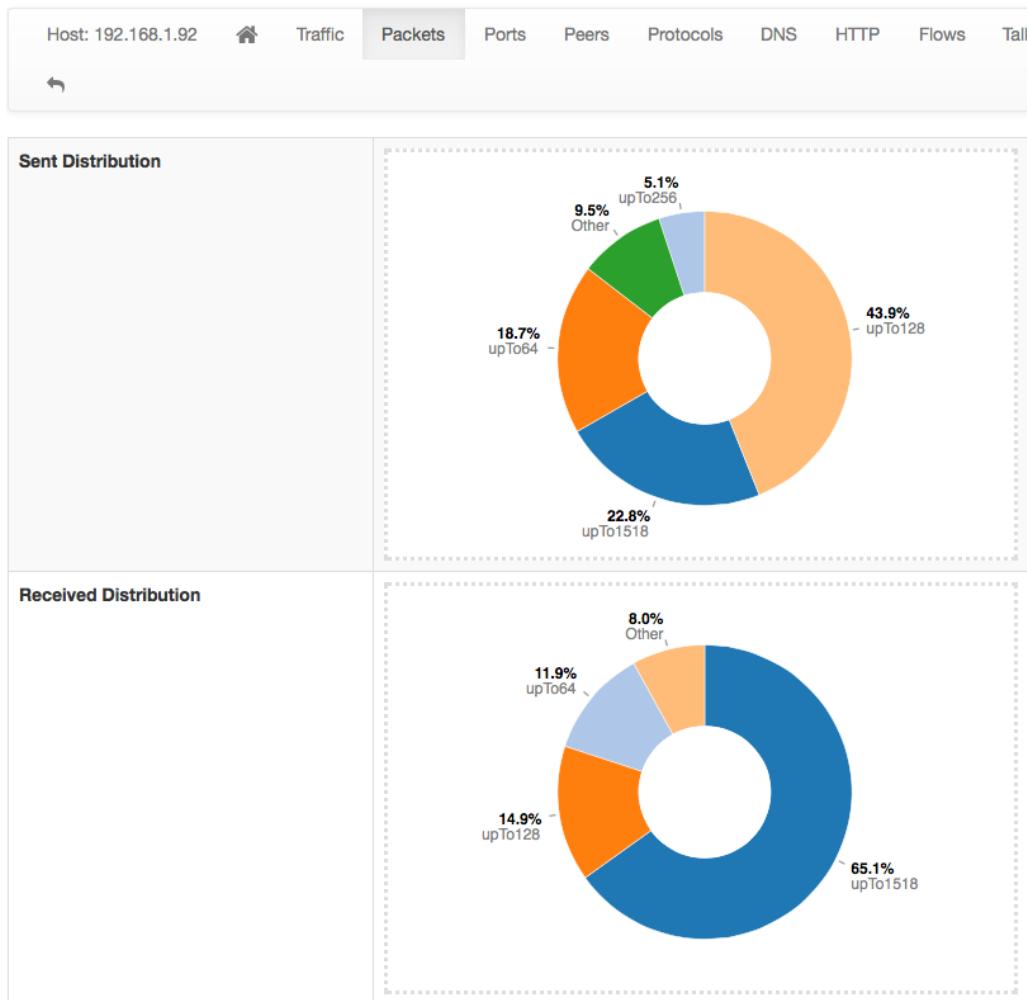


The Traffic View of the Host Details Page



Packets

Packets page provides pie charts with packet size distribution, both for sent and received packets.

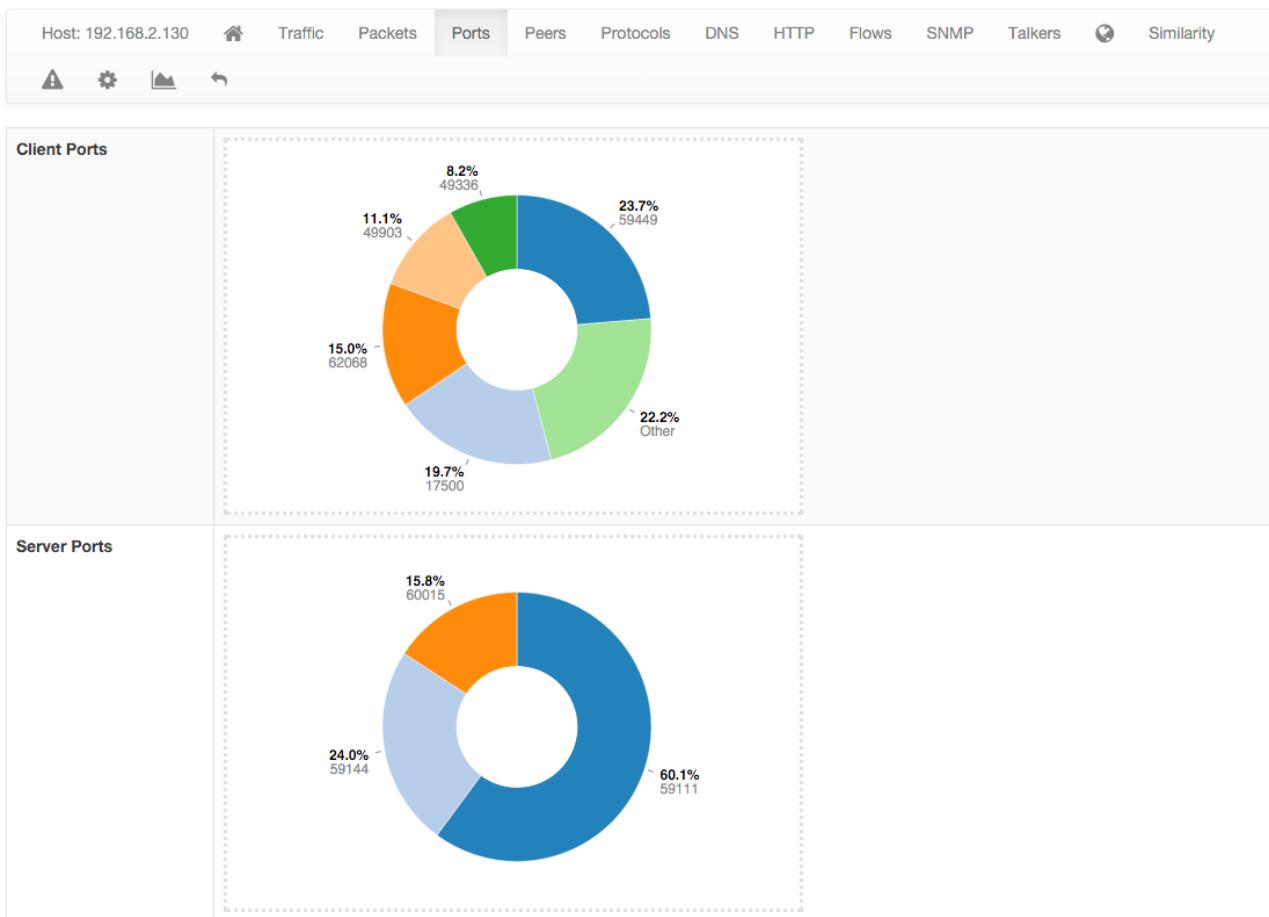


The Packets View of the Host Details Page



Ports

Ports page provides pie charts with traffic statistics grouped by port. A chart is available for client ports and another one is available for server ports.

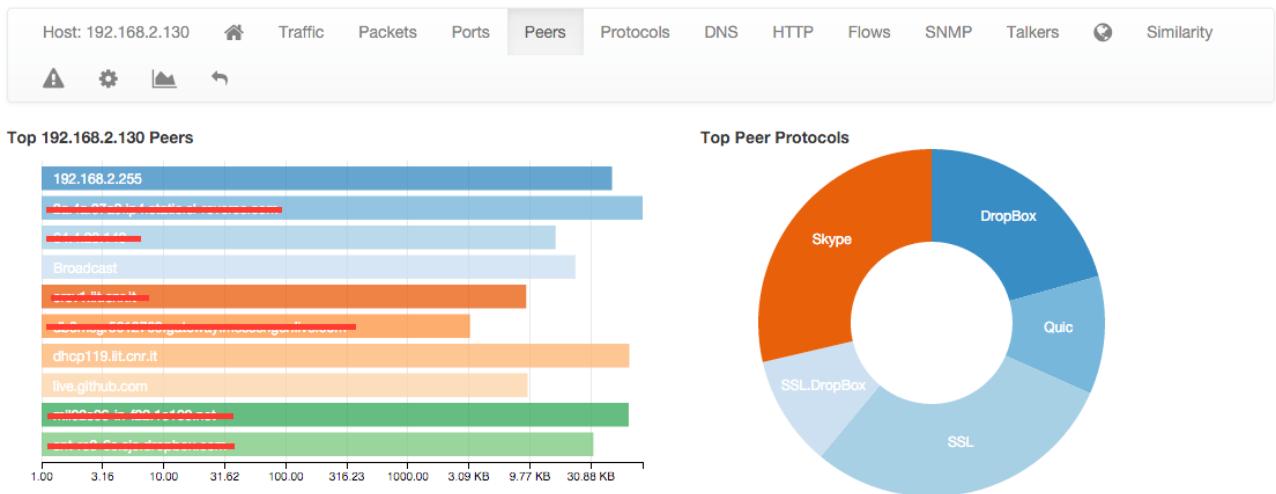


The Ports View of the Host Details Page



Peers

Peers page presents a graphical overview of top contacted peers and top protocols used. In the following screenshot some hosts are struck-through intentionally for privacy reasons. A table with top application per peer is shown below the graphical overview. Every information is clickable to allow the user to drill down and find insights.

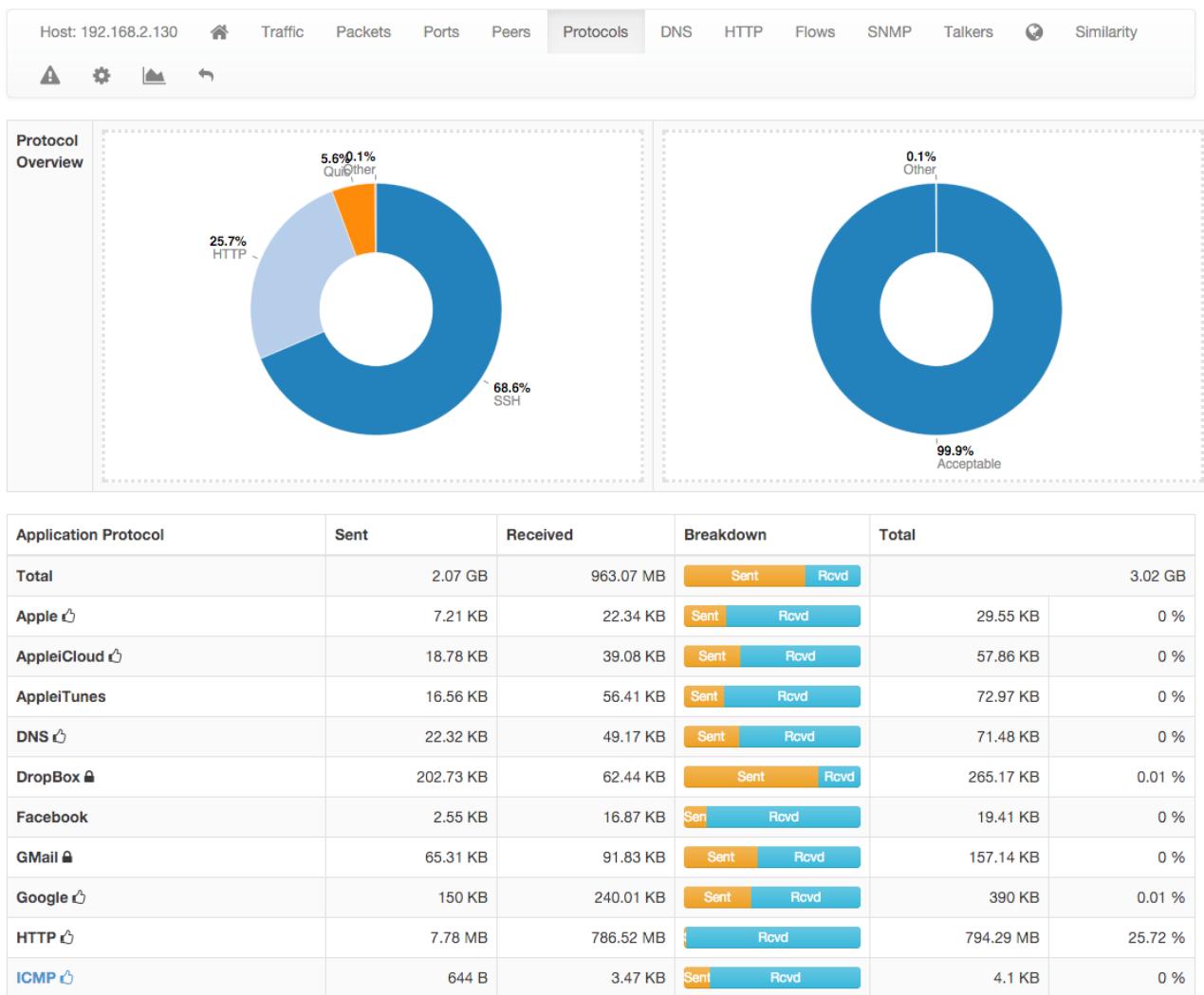


The Peers View of the Host Details Page



Protocols

Using the DPI information, this page provides in pie chart and tabular format the amount of traffic divided by application. An additional pie chart provides a statistics about protocol type. A click on the protocol name redirects the user to the page with detailed statistics about the selected protocol.

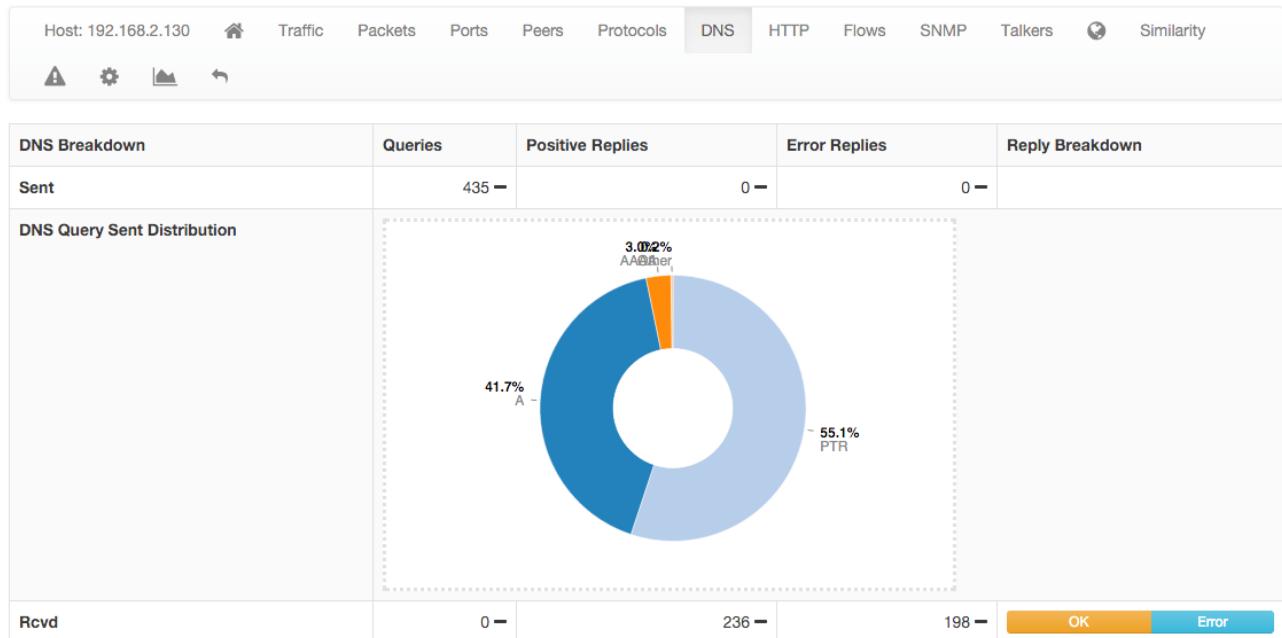


The Protocols View of the Host Details Page



DNS

The chart and the table displayed on this page report DNS statistics, such as the number of queries, their type (e.g., A, AAAA, PTR, and so on), and possible errors.

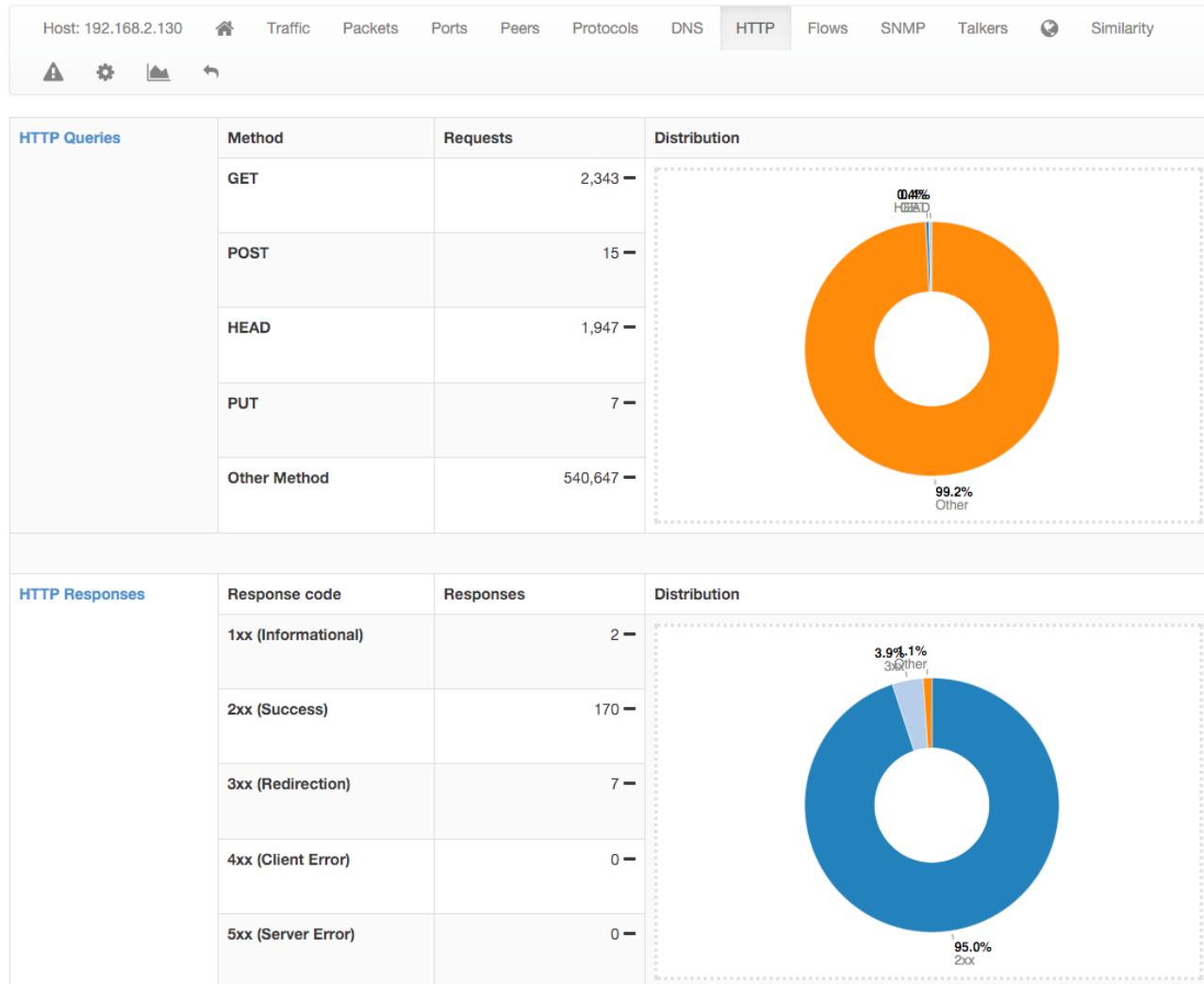


[The DNS View of the Host Details Page](#)



HTTP

This page provides information about the HTTP protocol in terms of requests done and responses received for each HTTP method, together with response codes. Counters are provided both as tables and pie charts. 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 a virtual server table.



The HTTP View of the Host Details Page

HTTP Responses	Response code	Responses	Distribution
	1xx (Informational)	0	
	2xx (Success)	0	
	3xx (Redirection)	0	
	4xx (Client Error)	0	
	5xx (Server Error)	0	

Virtual Hosts	Name	Traffic Sent	Traffic Received	Requests Served
	192.168.100.5 ↗	1.84 MB	0 Bytes	1,216

The HTTP View of the Host Details Page with Virtual Hosts



Flows

Flows page lists all active flows that have the selected host as an endpoint. A section of this manual discuss in greater detail the statistics shown for flows.

The screenshot shows the ntop interface with the 'Host' set to 192.168.2.130. The 'Flows' tab is selected. Below it, there's a table titled 'Active Flows' with one row. The columns are: Info, Application, L4 Proto, Client, Server, Duration, Actual Thpt, Total Bytes, and Info. The data row is: Info (Info icon), UbuntuONE (blue link), TCP, 192.168.2.130:60181, pyracantha.canonical... (blue link), :http, 19 sec, 42.49 Mbit ↑, 84.98 MB, and an empty Info field.

Active Flows

100 ▾

Info	Application	L4 Proto	Client	Server	Duration	Actual Thpt	Total Bytes	Info
Info	UbuntuONE ↗	TCP	192.168.2.130:60181	pyracantha.canonical... 🇺🇸 :http	19 sec	42.49 Mbit ↑	84.98 MB	

[The Flows View of the Host Details Page](#)

SNMP

SMNP page provides SNMP information for the selected host with all the standard SNMP traffic metrics.

SNMP Community	public	<input type="button" value="Save Community"/>
SysDescr	Linux ubuntu 3.13.0-37-generic #64~precise1-Ubuntu SMP Wed Sep 24 21:37:11 UTC 2014 x86_64	
SysUptime	2 days, 4 h, 18 min, 34 sec	
SysContact	Me	
SysName	ubuntu	
SysLocation	Sitting on the Dock of the Bay	
SysServices	72	

[The SMNP View of the Host Details Page](#)

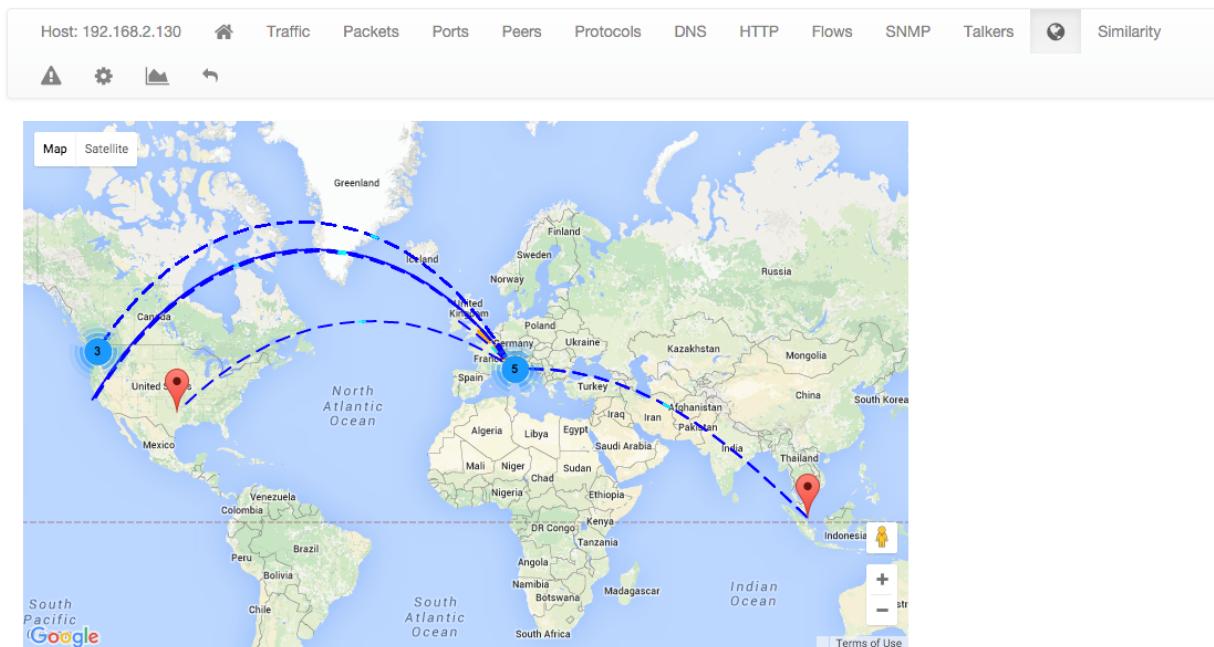


Talkers

Talkers page provides top talkers having active flows with selected host. Similarly to the Community edition dashboard, top talkers are laid out in a Sankey Diagram.

Geography

Geography page provides an interactive map that shows the selected hosts, its flows, and its peers.



The Geography View of the Host Details Page

Similarity

Similarity page displays the list of hosts that have traffic patterns that can be considered similar to those of the selected host. Similarity is defined using the Jaccard Coefficient⁵



The Similarity View of the Host Details Page

⁵ http://en.wikipedia.org/wiki/Jaccard_index



Alerts Configuration ⚠

Alerts Configuration page enables the user to set custom thresholds on multiple metrics, and to trigger alerts based on those thresholds. Alerts can be armed per total bytes, DNS traffic, P2P traffic or packets, in a fixed time interval. Available time intervals are 1 and 5 minutes, 60 minutes, and 1 day.

Every Minute	Every 5 Minutes	Hourly	Daily
Alert Function	Threshold		
bytes	> <input type="text"/>	Bytes delta (sent + received)	
dns	> <input type="text"/>	DNS traffic delta bytes (sent + received)	
p2p	> <input type="text"/>	Peer-to-peer traffic delta bytes (sent + received)	
packets	> <input type="text"/>	Packets delta (sent + received)	

Save Configuration [[Delete All Host Configured Alerts](#)]



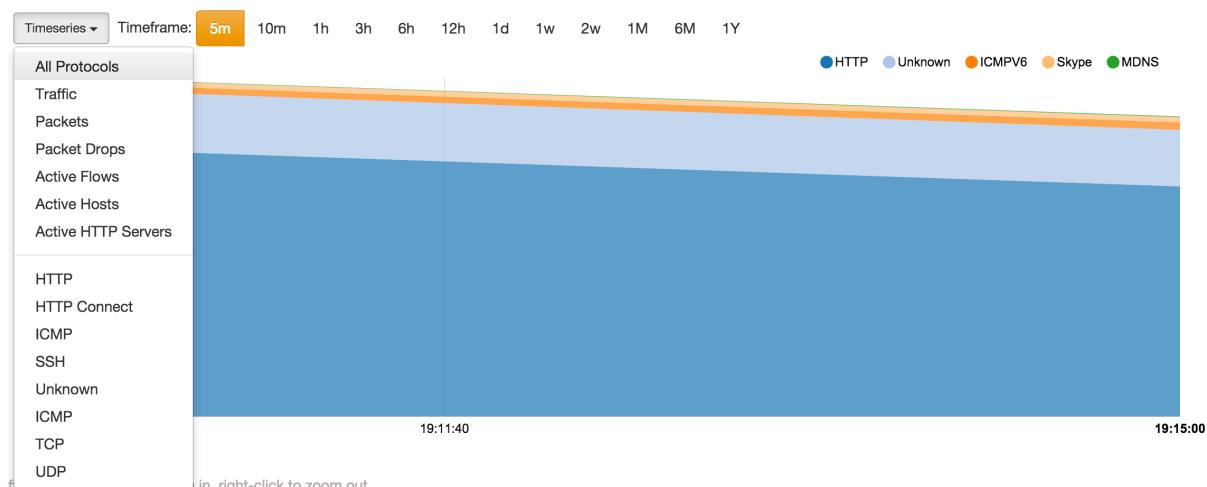
Statistics

Statistics page provides historical traffic statistics for the selected host. The user can choose to filter statistics on a protocol basis and display data in several formats (e.g., bytes, packets, flows, and so on).



Left-click on the chart to zoom in, right-click to zoom out.

The Statistics View of the Host Details Page



The Dropdown menu in The Statistics View of the Host Details Page



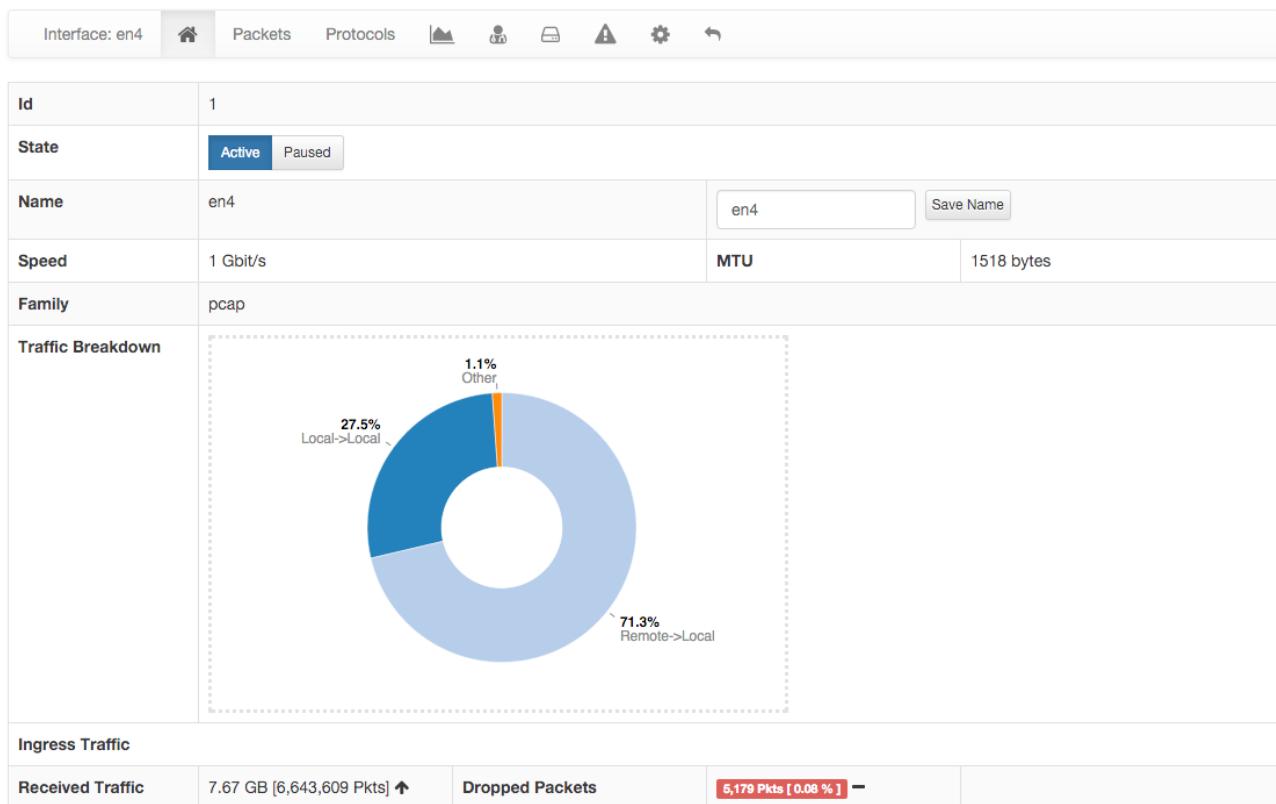
Interfaces

The Interfaces dropdown menu entry in the top toolbar contains lists all the interfaces that are currently monitored by ntopng. Among all interfaces listed, one has a check mark that indicates the interface is currently selected. Every data and information shown in ntopng web GUI relates to the currently selected interface. Any interface listed can be selected simply by clicking on its name.



The Interfaces Dropdown Menu

The dropdown menu is only used to switch between selected interfaces, it is also used to actually see interface traffic statistics. Interface traffic statistics can be accessed by clicking on the currently selected interface. A contextual menu with multiple options and badges appear right below the top toolbar. Menu entries are discussed below.



The Home View of the Interface Details Page

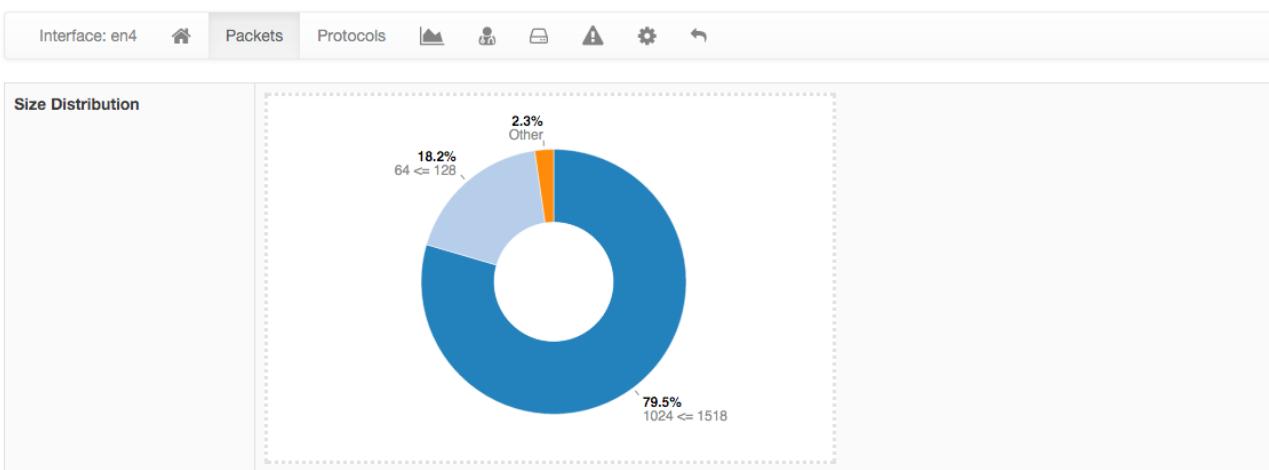


Home

In the Home page it is possible to view general interface information, such as Id (a unique integer identifier ntopng assigns to each monitored interface), family (e.g., pcap), and the overall traffic counters in bytes. It is possible to customize the interface name just by writing a custom name into the Name textbook and clicking on “Save Name”. Interface monitoring can be temporarily paused from the ‘State’ toggle buttons.

Packets

Packets page shows a pie chart of packets size distribution.

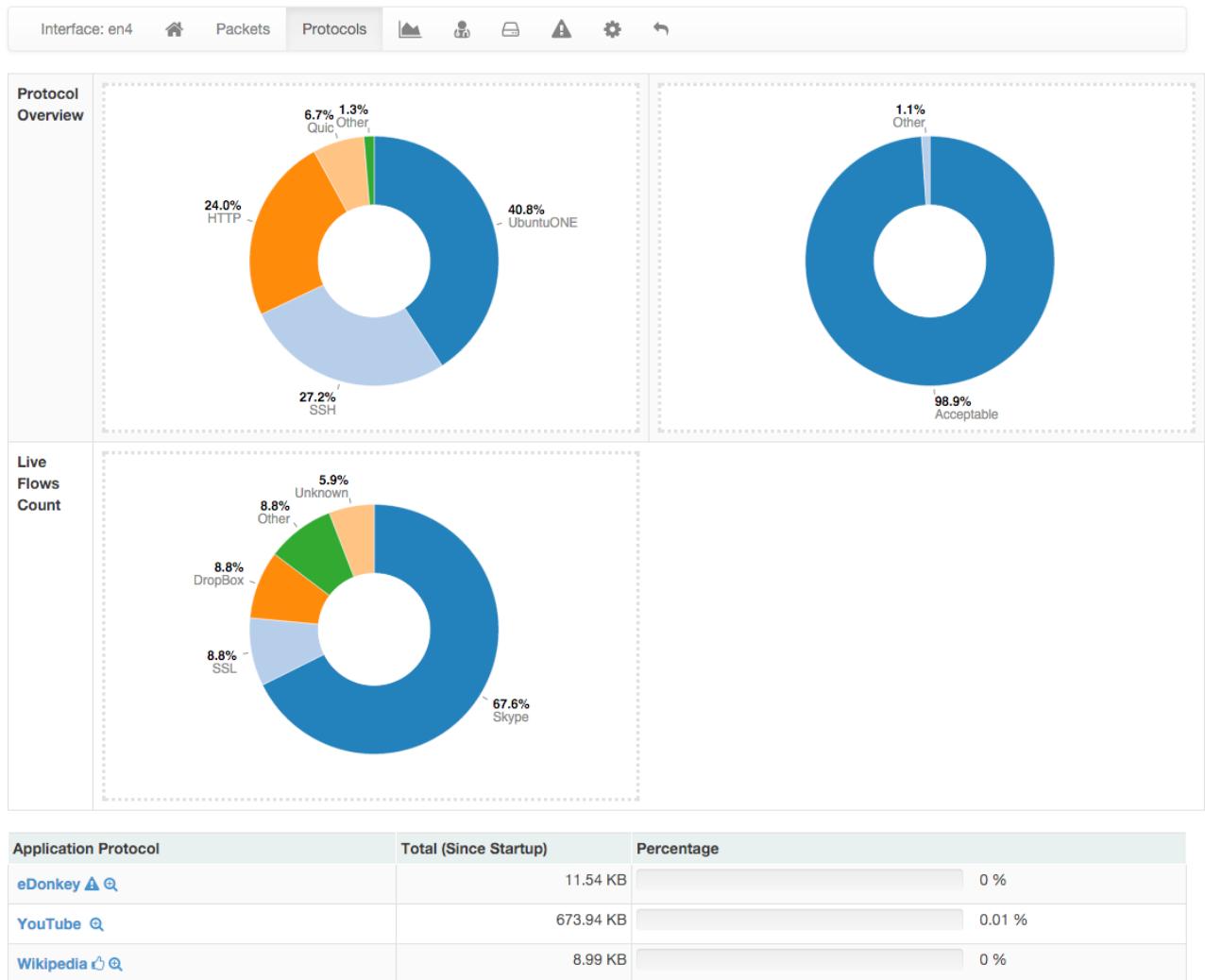


The Packets View of the Interface Details Page



Protocols

Protocols page provides three pie charts and a specific table with nDPI-detected protocols for the selected interface.



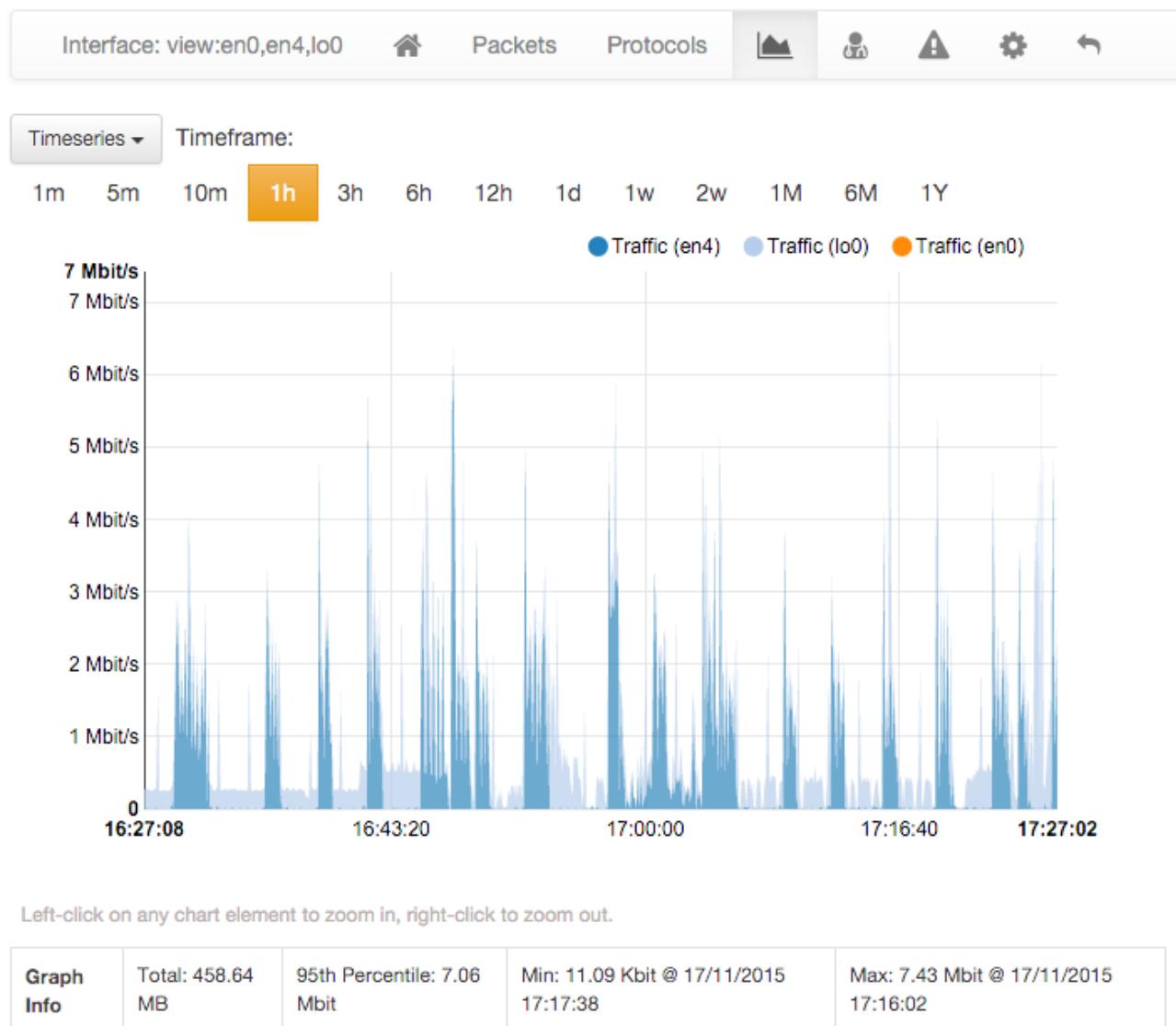
The Protocols View of the Interface Details Page

In the two top pie charts ntopng shows the application distribution and its categorization. The bottom pie chart shows nDPI-detected applications for currently active flows. All labels are clickable and point to detailed statistics pages. Below pie charts there is a list of protocols detected with the corresponding total traffic, both in absolute terms and as a percentage of the total traffic. By selecting any Application Protocol, it is possible to display a statistics page with temporal charts for that protocol. Similarly, by clicking on the magnifying lens icon, it is possible to display all active flows for that protocol.



Statistics

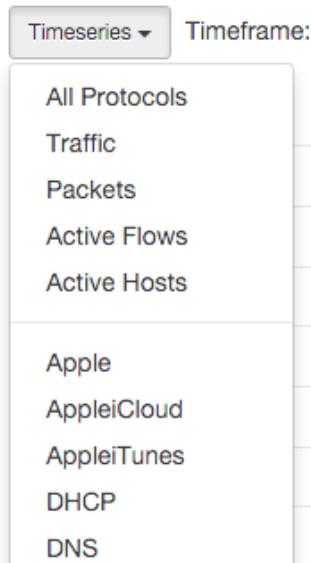
Statistics page provides historical traffic statistics for the selected interface. The user can choose to filter statistics on a protocol basis and display data in several formats (e.g., bytes, packets, flows, and so on). In the Professional Version of ntopng, traffic for interface views in shown as stacked per physical interface. Physical interface visualization can be toggled by clicking on the colored dot just left of interface name.



The Statistics View of the Interface Details Page (Professional Version)

The time series span can be adjusted by selecting values from 5 minutes up to 1 year. Moreover, drill-down is possible by clicking on the time series itself. Every click zooms the chart in, centering the time series around the clicked point.

Moreover, time series shown can be chosen via the dropdown menu labelled ‘Timeseries’. For example, it is possible to visualize all or just one protocol, traffic, packets, active hosts and flows, and so on. Ntopng is Vlan aware, hence if several Vlans are detected, traffic is accounted also on a Vlan basis.



The Dropdown Time Series Menu in the Statistics View of the Interface Details Page

A Minute Traffic Statistics appears left of the main statistics chart when the selected interface is not a view. Similarly, an historical flows table is present below the main chart when ntopng is started with the -F switch. This historical table shows flows data that have been recorded and dumped during the selected observation period.

	IPv4	IPv6	IPv4 Top Flows [17/11/2015 10:14:00 - 17/11/2015 13:14:00]									5 ▾
	Application	L4 Proto	Client	Server	Begin	End	Bytes	Info	Avg Thpt			
Info	HTTP	TCP	192.168.2.130:65401	service01.crazynetwork.l...:http	17/11/2015 13:08:40	17/11/2015 13:13:42	905943994	mirror.crazynetwork.it	23.92 Mbit			
Info	UbuntuONE	TCP	192.168.2.130:65378	acai.canonical.com:http	17/11/2015 13:08:40	17/11/2015 13:13:42	684944111	releases.ubuntu.com	18.08 Mbit			
Info	UbuntuONE	TCP	192.168.2.130:60181	pyracantha.canonical.com...:http	17/11/2015 11:05:33	17/11/2015 11:05:38	16635410	releases.ubuntu.com	22.18 Mbit			

The Historical Flows Table of the Interface Details Page Statistics View

Traffic Profiles (Professional Version)

TODO: describe traffic profiles

Packet Dump

Statistics 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 by 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).

The screenshot shows the ntopng web interface with a yellow header bar. The main menu includes Home, Flows, Hosts, Protocols, Interfaces (selected), and a search bar for 'Search Host'. Below the menu, the interface is titled 'Interface: eth0' and shows tabs for Overview, Packets, Protocols, Historical Activity, and Packet Dump (selected). The 'Packet Dump' section contains several configuration options:

- Packet Dump To Disk**: Includes checkboxes for 'Dump Traffic To Disk' and 'Dump Unknown Traffic To Disk'.
- Packet Dump To Tap**: Includes a checkbox for 'Dump Traffic To Tap (tap0)'.
- Sampling Rate**: A dropdown set to '1 : 1' with a 'Save' button. A note below states: 'NOTE: Sampling rate is applied only when dumping packets caused by a security alert (e.g. a volumetric DDoS attack) and not to those hosts/flows that have been marked explicitly for dump.'
- Dump To Disk Parameters**:
 - Max Packets per File**: Set to 3000000 with a 'Save' button. A note says: 'Maximum number of packets to store on a pcap file before creating a new file.'
 - Max Duration of File**: Set to 300 sec with a 'Save' button. A note says: 'Maximum pcap file duration before creating a new file. NOTE: a dump file is closed when it reaches first the maximum size or duration specified.'

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:

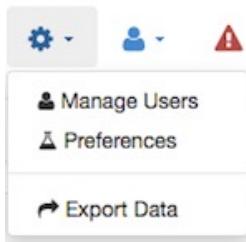


Figure 79 - Setting Menu

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	<button>Manage</button>

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.

Export JSON Data **Reset Form**

Figure 83 - Export Data Page

Administration Menu



Figure 84 - User Icon

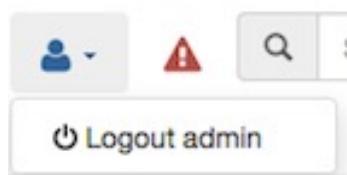


Figure 85 - User Menu

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. It displays a table with columns: Action, Date, Severity, Type, and Description. The table lists 64 rows of alerts, all categorized as 'Error' and type 'TCP SYN Flood'. The descriptions detail various SYN flood attacks on host 192.168.100.5 and 192.168.100.1 from other hosts like 192.168.100.1, 192.168.100.5, and 192.168.100.100. The interface includes navigation buttons at the bottom and a search bar at the top.

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]

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

A search bar with a magnifying glass icon and the placeholder text '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.