ntopng User's Guide

Version 2.3

June 2016

Index

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 is possible to modify its behavior by customizing 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>
```

Section "Command Line Options" of this guide thoroughly discuss any available option.

The ntopng Configuration File

Command line options can be grouped in a plain text file, that is typically named `ntopng.conf`. Note that any name is acceptable except when ntopng is run as a daemon in which case `ntopng.conf` file name must be used.

Options in the configuration file must be reported one per line. Comment lines are accepted as well and have to be prefixed with the '#' sign. Option name and option value must be separated by the '=' sign. The latter sign is necessary even for options that doesn't require a value. For example, to disable interface promiscuous mode, one would use `--no-promisc` when starting ntopng directly from the command line or would add a line `--no-promisc=` in the configuration file when starting ntopng as a daemon.

An example of a configuration file is the following

```
$ cat /etc/ntopng/ntopng.conf
-G=/var/tmp/ntopng.pid
--daemon=

# Listen on localhost:3000 only
--http-port=:3000

# Use prefix due to nginx proxy
--http-prefix="/ntopng"

# Everybody's admin
#--disable-login=1

# Do not resolve any names
--dns-mode=3

# Limit memory usage
--max-num-flows=200000
--max-num-hosts=250000
--sticky-hosts=none

# Dump flows to MySQL
--dump-flows=mysql;localhost;ntopng;flows;ntopng;xxx

# Dump hosts to sqlite files
--dump-hosts=all

#--verbose
```

Running ntopng as a Daemon

Ntopng can be run in daemon mode on unix systems and optionally be run automatically on system startup. Daemon execution and status are controlled using the script

```
/etc/init.d/ntopng
```

The script is installed automatically on unix systems as it is part of any standard ntopng installation procedure.

Daemon Configuration File

Ntopng configuration file is required when running it as a daemon. The configuration file has to be named `ntopng.conf` and must be placed under

```
/etc/ntopng/
```

The interested reader can find above and example of a configuration file.

Automatic Daemon Startup on Boot

In order to launch ntopng daemon automatically on system startup, an empty file `ntopng.start` must be created in the same directory of the configuration files. Therefore, the directory will contain both the configuration and the startup files

```
root@devel:/etc/ntopng# ls -lha
total 28K
drwxr-xr-x   2 root root 4.0K Mar 17 15:44 .
drwxr-xr-x 117 root root  12K Mar 11 12:16 ..
-rw-r--r--   1 root root  211 Mar 15 17:54 ntopng.conf
-rw-r--r--   1 root root    0 Mar 17 15:44 ntopng.start
```

Daemon Control

ntopng daemon is controlled with the script `/etc/init.d/ntopng`. The script accepts different options. Calling the script without options yields the following brief help

```
deri@devel 204> sudo /etc/init.d/ntopng
Usage: /etc/init.d/ntopng {start|force-start|stop|restart|status}
```

The options and the usage of the daemon control script is discusse below.

start
This option is used to start the ntopng daemon

```
deri@devel 204> /etc/init.d/ntopng start
 * Starting ntopng
   ...done.
```

force-start
Equivalent to start.

stop
This option is used to stop an ntopng daemon instance. For example

```
deri@devel 204> /etc/init.d/ntopng stop
 * Stopping ntopng
   ...done.
```

restart
This option causes the restart of a daemon associated to a given interface, e.g.,

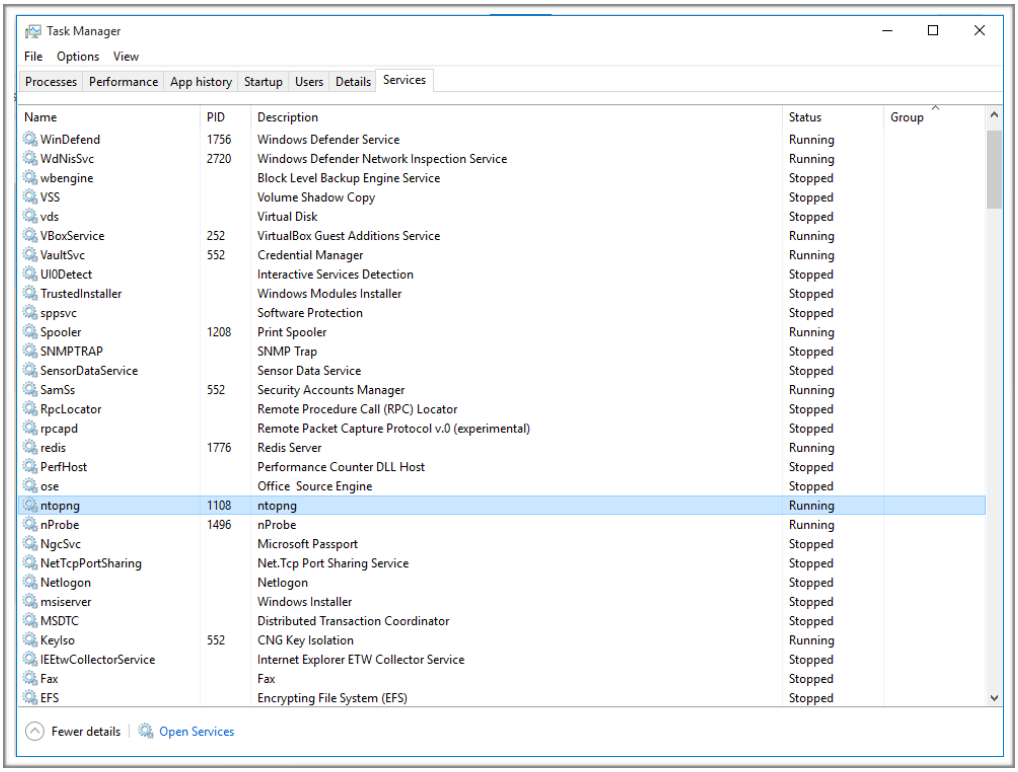
```
deri@devel 204> /etc/init.d/ntopng restart
 * Stopping ntopng
 * Starting ntopng
   ...done.
```

status
This options prints the status of a daemon associated to a given interface, e.g.,

```
deri@devel 204> /etc/init.d/ntopng status
ntopng running as 5623
```

Running ntopng on Windows

Ntopng can be run either as service or as application (i.e. you can start it from cmd.exe). The ntopng installer registers the service and automatically starts is as shown below.



The Windows Services Manager

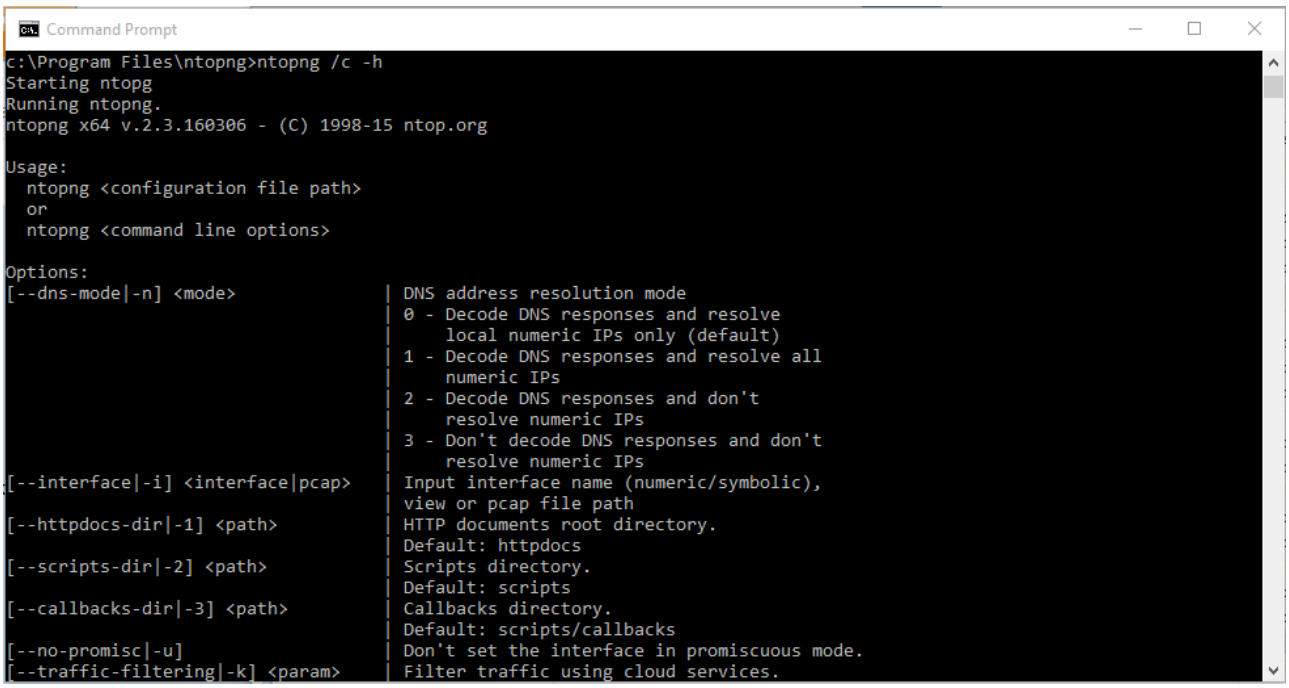
In order to interact with ntopng from the command line, fire up a Windows Commands Promt and navigate to the ntopng installation directory. You may need to execute the commands promo with Administrator privileges. Commands are issued after a /c that stands for “console”. For example to display the inline help it suffices to run

```
ntopng /c -h
```

Specify Monitored Interfaces

As network interfaces on Windows can have long names, a numeric index is associated to the interface in order to ease the ntopng configuration. The association interface name and index is shown in the inline help.

```
c:\Program Files\ntopng>ntopng /c -h
Starting ntopg
Running ntopng.
ntopng x64 v.2.3.160306 - (C) 1998-15 ntop.org
```



The Windows Command Promt

```
[…]

Available interfaces (-i <interface index>):
   1. Intel(R) PRO/1000 MT Desktop Adapter
        {8EDDEFE3-D6DB-4F9B-9EDF-FBC0BFF67F3C}
[…]
```

In the above example the network adapter Intel(R) PRO/1000 MT Desktop is associated with index 1. To select this adapter ntopng needs to be started with –i 1 option.

Execution as a Windows Service

Windows services are started and stopped using the Services application part of the Windows administrative tools. When ntopng is used as service, command line options need to be specified at service registration and can be modified only by removing and re-adding the service. The ntopng installer registers ntopng as a service with the default options. The default registered service options can be changed using these commands:

ntopng /r	Remove the service
ntopng /i <new set of options>	Install the service with the specified options.

In a Commands Promt:

```
c:\Program Files\ntopng>ntopng /r
ntopng removed.

c:\Program Files\ntopng>ntopng /i -i 1
ntopng installed.
NOTE: the default password for the 'admin' user has been set to 'admin'.
c:\Program Files\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 --help
ntopng x86_64 v.2.3.160616 - (C) 1998-2016 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
[--install-dir|-t] <path>           | Set the installation directory to <dir>.
                                    | Should be set when installing ntopng
                                    | under custom directories
[--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.
[--traffic-filtering|-k] <param>    | Filter traffic using cloud services.
                                    | (default: disabled). Available options:
                                    | httpbl:<api_key>        See README.httpbl
[--http-port|-w] <[addr:]port>      | HTTP. Set to 0 to disable http server.
                                    | Addr can be any valid ipv4 (e.g., 192.168.1.1)
                                    | or ipv6 (e.g., [3ffe:2a00:100:7031::1]) address.
                                    | Surround ipv6 addresses with square brackets.
                                    | Prepend a ':' without addr before the port
                                    | to listen on the loopback address.
                                    | Default port: 3000
                                    | Examples:
                                    | -w :3000
                                    | -w 192.168.1.1:3001
                                    | -w [3ffe:2a00:100:7031::1]:3002
[--https-port|-W] <[:]https port>   | HTTPS. 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]     | Disable host persistency in the Redis cache
[--redis|-r] <host[:port][@db-id]>  | Redis host[:port][@database id]
[--user|-U] <sys user>              | Run ntopng with the specified user
                                    | instead of nobody
[--dont-change-user|-s]             | Do not change user (debug only)
[--shutdown-when-done]              | Terminate when a pcap has been read (debug only)
[--zmq-collector-mode]              | Force ZMQ sockets to operate in collector mode. If
                                      | used nprobe must use --zmq-probe-mode so that it
can
                                    | behave as a probe.
```

```
--zmq-encrypt-pwd <pwd>             | Encrypt the ZMQ data using the specified password
[--disable-autologout|-q]           | Disable web interface logout for inactivity
[--disable-login|-l] <mode>         | Disable user login authentication:
                                    | 0 - Disable login only for localhost
                                    | 1 - Disable login only for all hosts
[--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]               | Disable alerts generation
[--packet-filter|-B] <filter>       | Ingress packet filter (BPF filter)
[--dump-flows|-F] <mode>            | 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|-I] <endpoint>      | Export flows using the specified endpoint.
[--dump-hosts|-D] <mode>            | Dump hosts policy (default: none).
                                    | Values:
                                    | all    - Dump all hosts
                                    | local  - Dump only local hosts
                                    | remote - Dump only remote hosts
[--sticky-hosts|-S] <mode>          | 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
--hw-timestamp-mode <mode>          | 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
--capture-direction                 | Specify packet capture direction
                                    | 0=RX+TX (default), 1=RX only, 2=TX only
--online-license-check              | Check license online
[--enable-taps|-T]                  | Enable tap interfaces used to dump traffic
[--http-prefix|-Z] <prefix>         | HTTP prefix to be prepended to URLs. This is
                                    | useful when using ntopng behind a proxy.
[--instance-name|-N] <name>         | Assign an identifier to the ntopng instance.
[--community]                       | Start ntopng in community edition (debug only).
[--check-license]                   | Check if the license is valid.
[--check-maintenance]               | Check until maintenance is included in the license.
[--verbose|-v]                      | Verbose tracing
[--version|-V]                      | Print version and quit
[--print-ndpi-protocols]            | Print the nDPI protocols recognized di ntopng
[--help|-h]                         | Help

Available interfaces (-i <interface index>):
   1. en0
   2. p2p0
   3. awdl0
   4. bridge0
   5. utun0
   6. en1
   7. en2
```

```
8. lo0
9. gif0
10. stf0
```

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 though 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>/

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. All the command line options can be reported in the configuration file, one per line. Options must be separated from their values using a '=' sign. Comment lines starting with a '#' sign are allowed as well.

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.

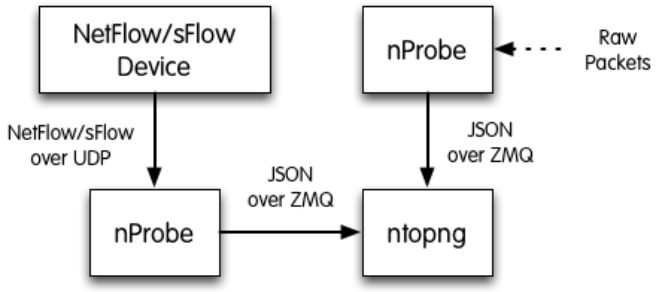
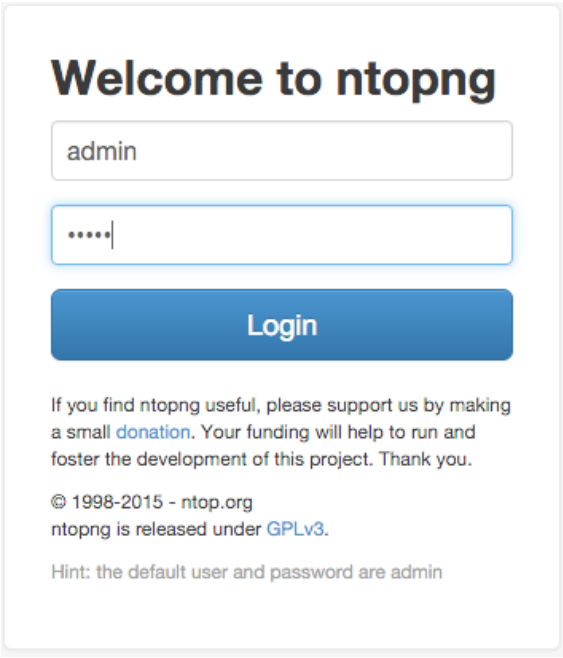


Figure 1 - ntopng/nprobe setup

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

The ntopng Web GUI

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.



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.

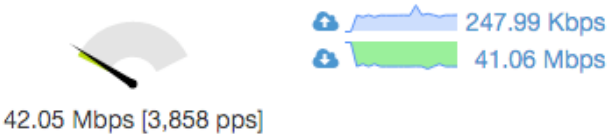
The Header Bar

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).

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

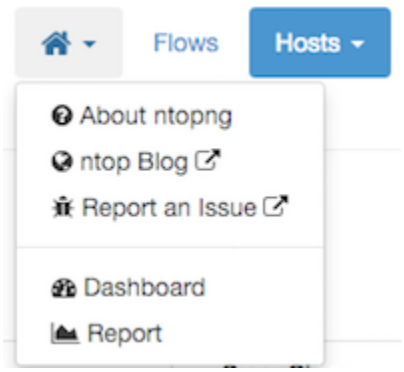
Gauge scale is calculated according to physical interfaces features. It is not always possible to determine maximum nominal interfaces speed. For this reason, scale can me manually configured simply by clicking on the gauge. Changes will be automatically saved to persistent storage.

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.

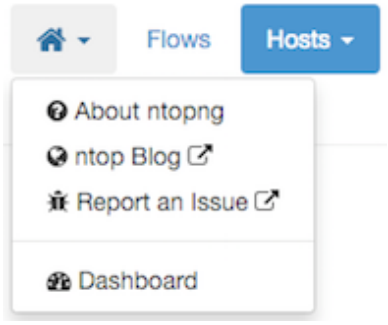
The Right Side of the Footer Bar

Home Menu

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



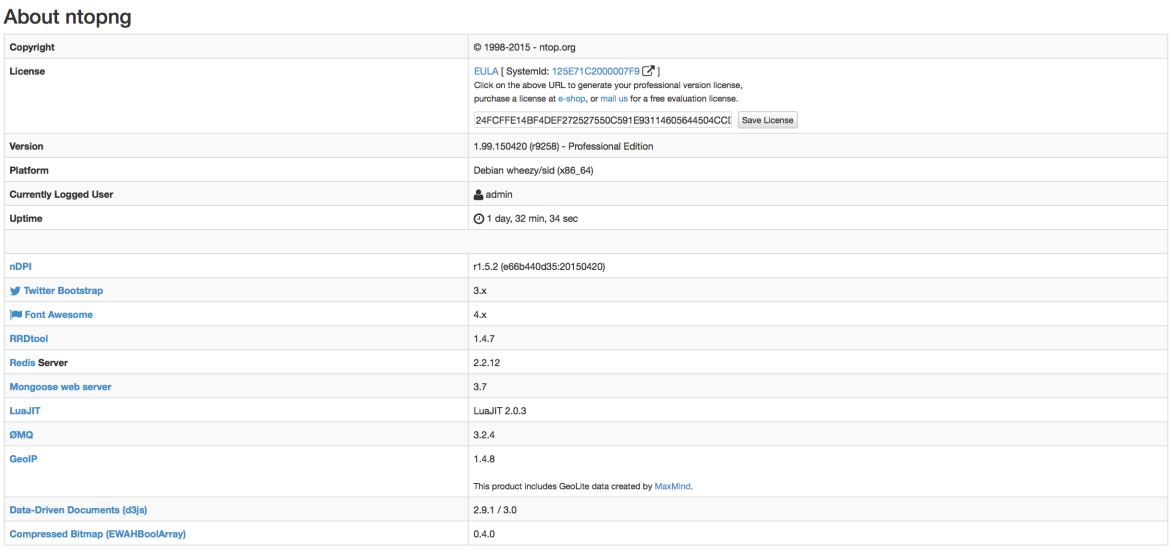
Professional Version Home Menu



Community Version Home Menu

About ntopng

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



The ‘About ntopng’ Page

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://github.com/ntop/ntopng/issues* page where you can report specific bug you discovered.

Dashboard

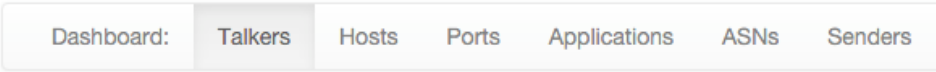
Provides a shortcut to default dashboard page of ntopng. The dashboard is discussed in greater detail in the following section.

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.

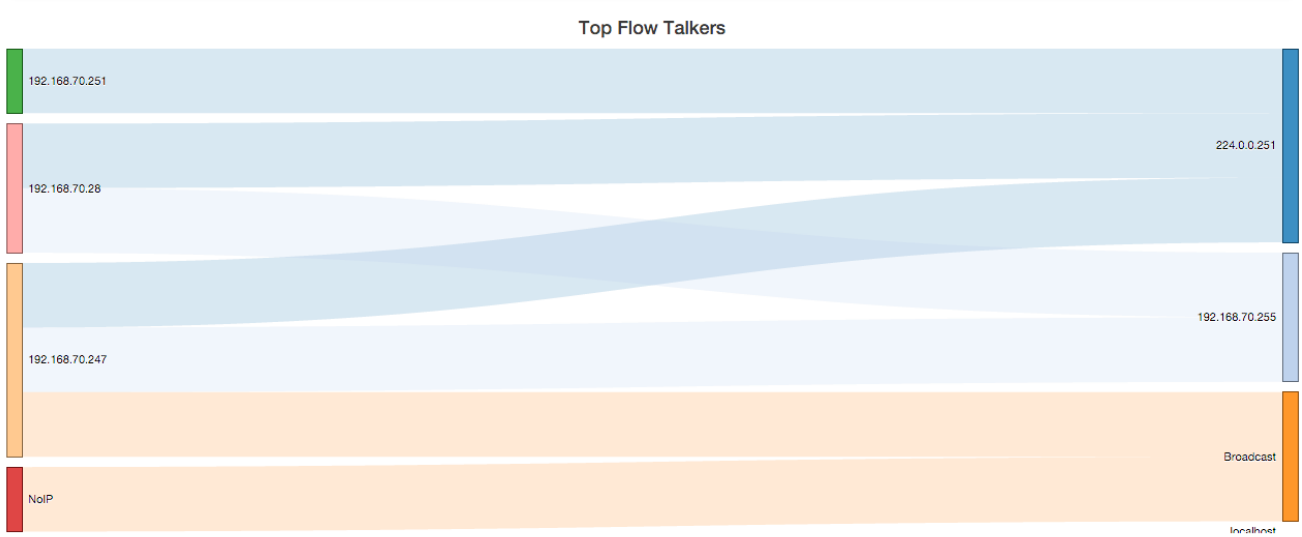
Dashboard in the Community Version

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

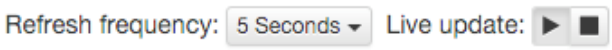


Diagram Refresh Settings

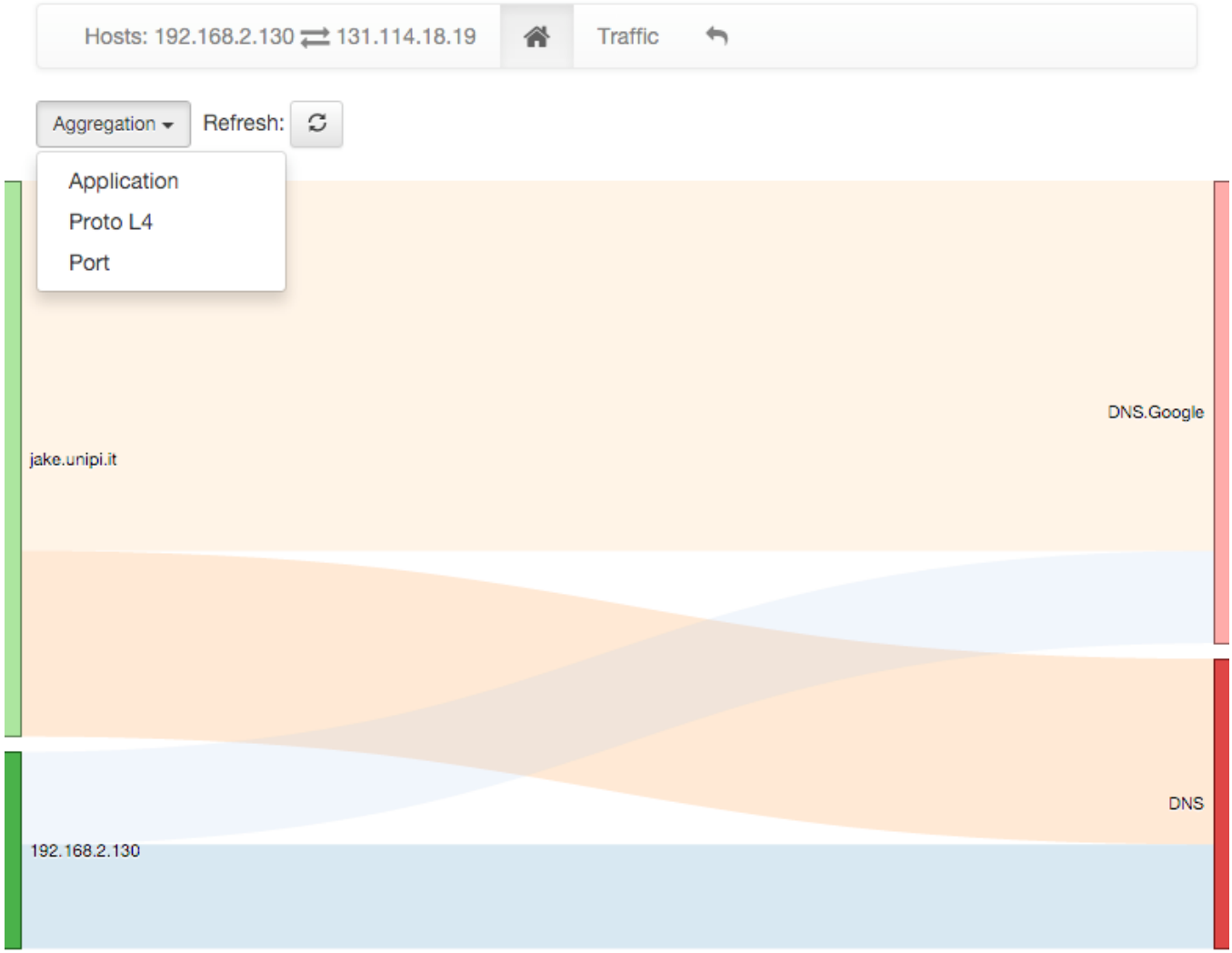
The Sankey diagram displays hosts currently active on the monitored interface or interface view. Host pairs are joined together by colored bars representing flows. The client host is always placed in the left edge of the bar. Similarly, the server is placed on the right. Bar width is proportional to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

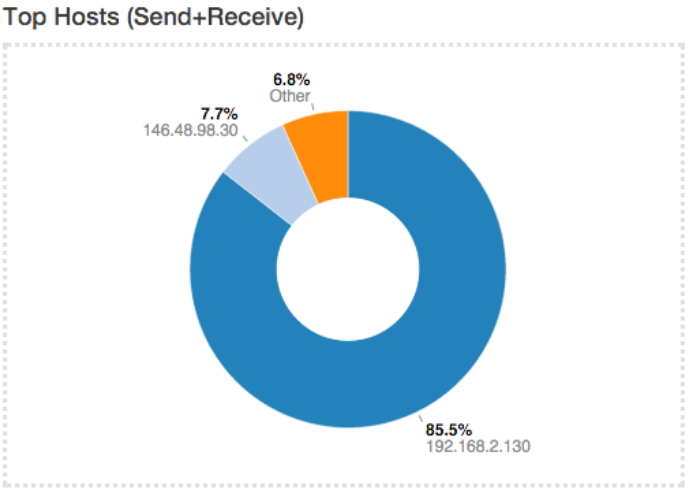


Pairwise Host Comparison

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.

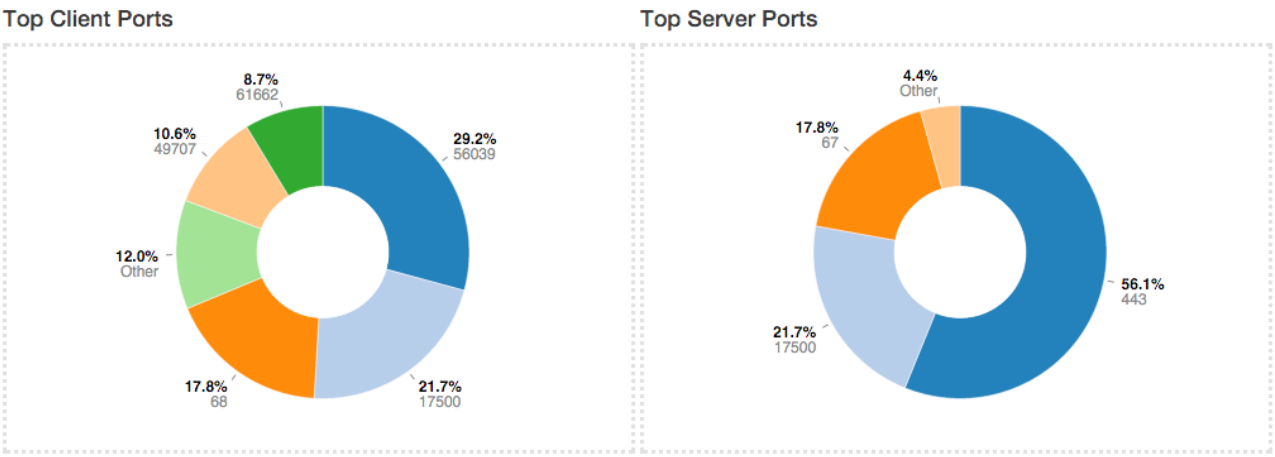
The pie chart is refreshed automatically.



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.

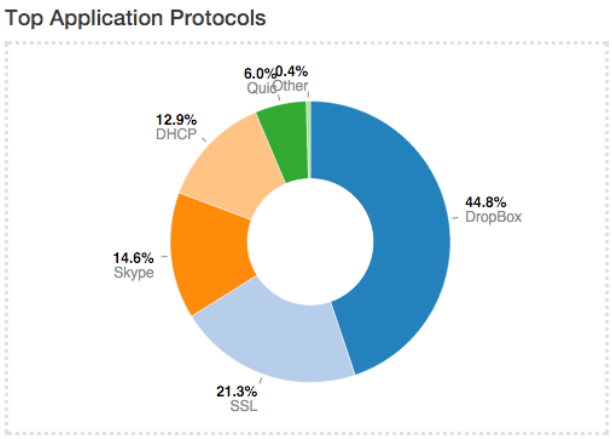


Pie Chart of Top Client and Server Ports

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 ntopn nDPI engine. Protocols that cannot be identified are marked as Unknown.

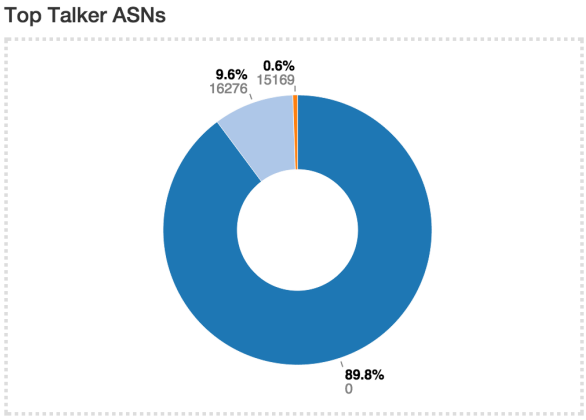


Pie Chart of Top Applications

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)

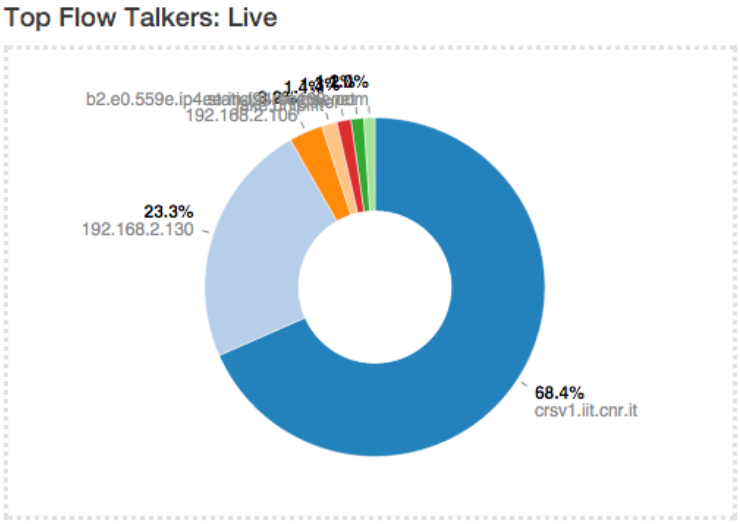
ASNs view provides a pie chart representation of the traffic grouped by Autonomous System (AS). An AS is either a single network or a group of networks, controlled by a network administrator on behalf of a single administrative entity (such as a university, a business enterprise, or a business division). 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.



Pie Chart of Top ASNs

Senders

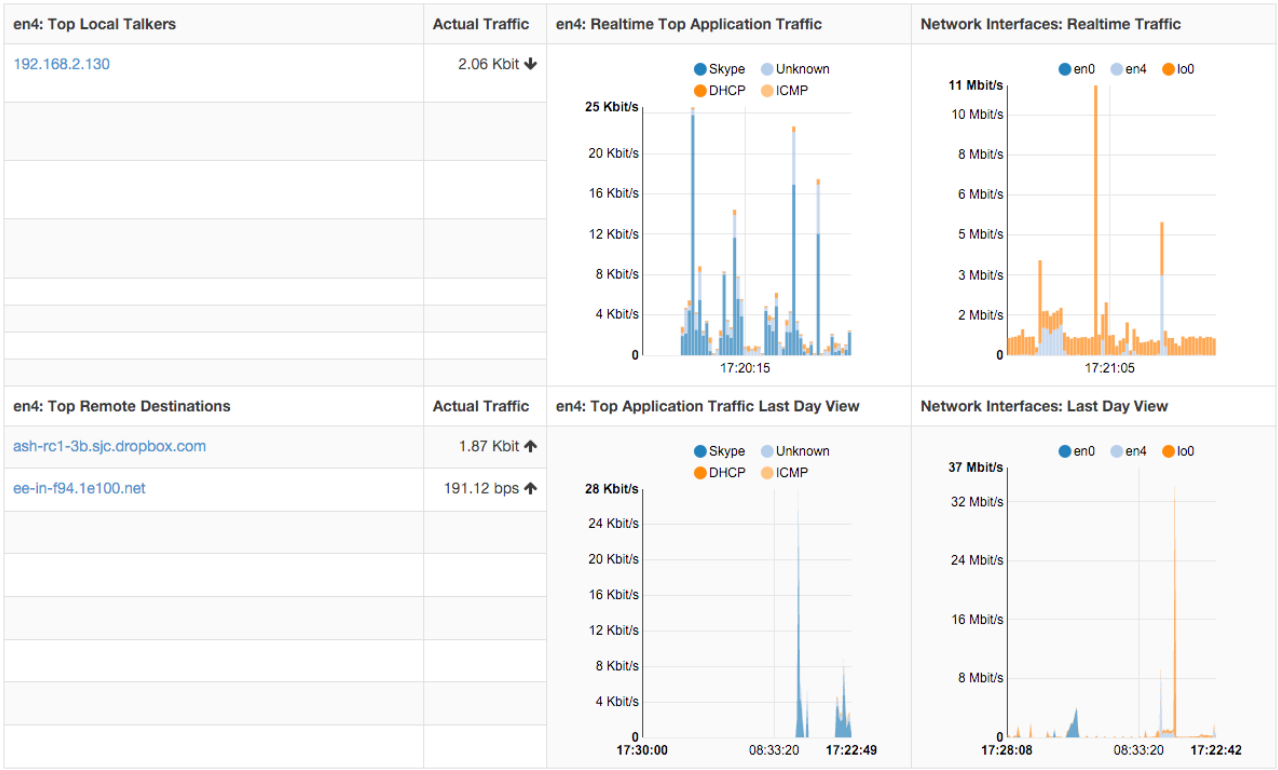
Senders view provides a pie chart representation of top flow senders currently active. This graph shows the percentage of traffic being sent by endpoints either on local or remote networks.



Pie Chart of Top Senders

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 chars are kept updated by ntopng.



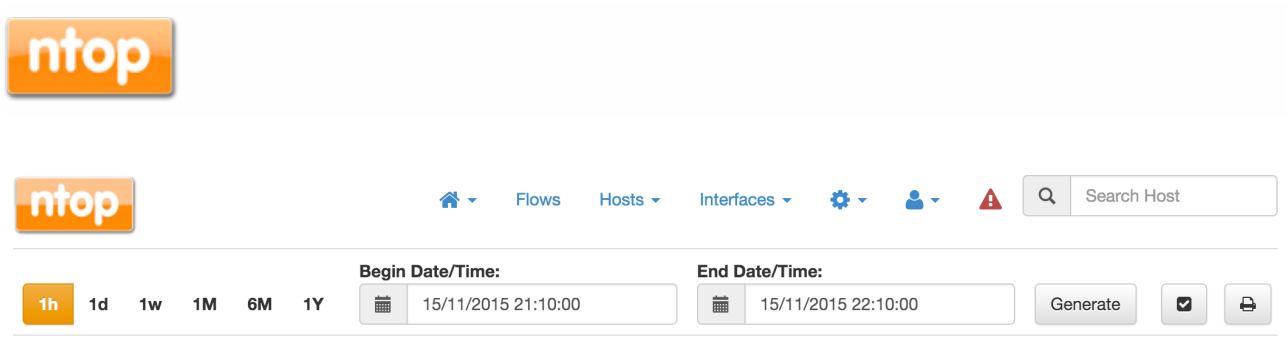
The right part of the dashboard displays realtime and last-day charts of Top Applications and Network Traffic. In case a network interface view is selected, then network traffic is shown on a per physical-interface basis. Items shown in each chart can be dynamically toggled simply by clicking on the corresponding coloured 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 that indicates whether the traffic for such host has increased/decreased since the last web page update.

Each host show can be clicked to access its 'Host Details' page. Next to a host you can find a badge enclosing a number: it indicates how many virtual HTTP servers the host features.

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

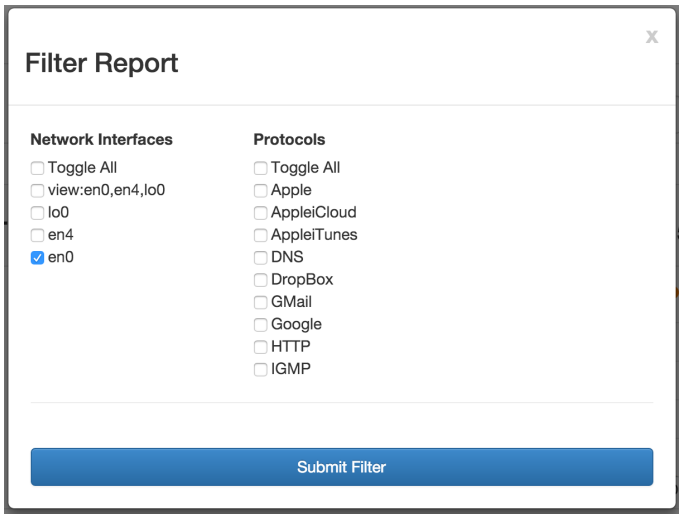


The Top of the Report Page

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.

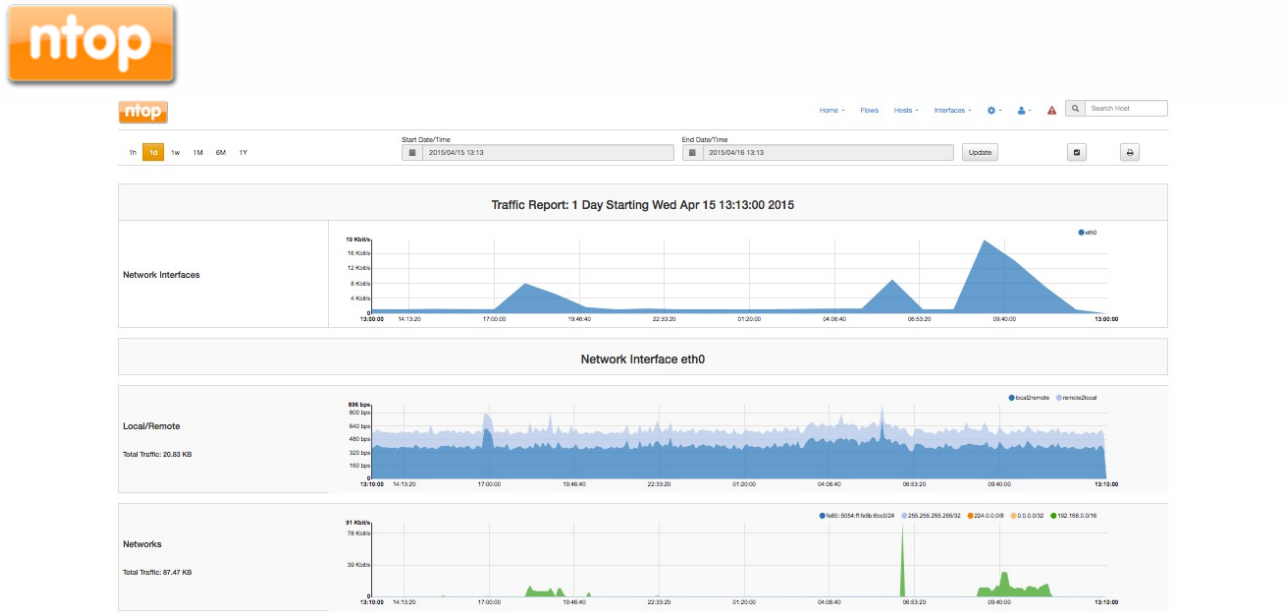
Exact temporal intervals can be chosen using the two dropdown date time pickers in the center. The first and the second pickers are used to specify the start and the end of a custom report, respectively. Once dates and times have been chosen, the report is obtained by clicking on 'Generate'.

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

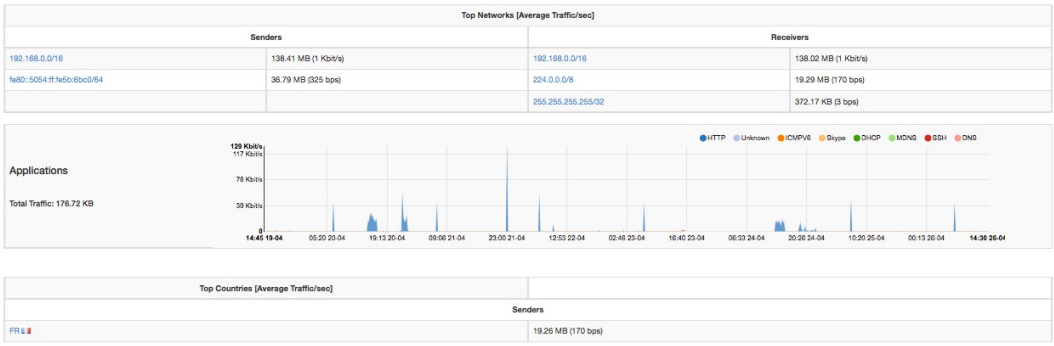


Report Filter Overlay

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



Generated Report - Network Interfaces and Traffic

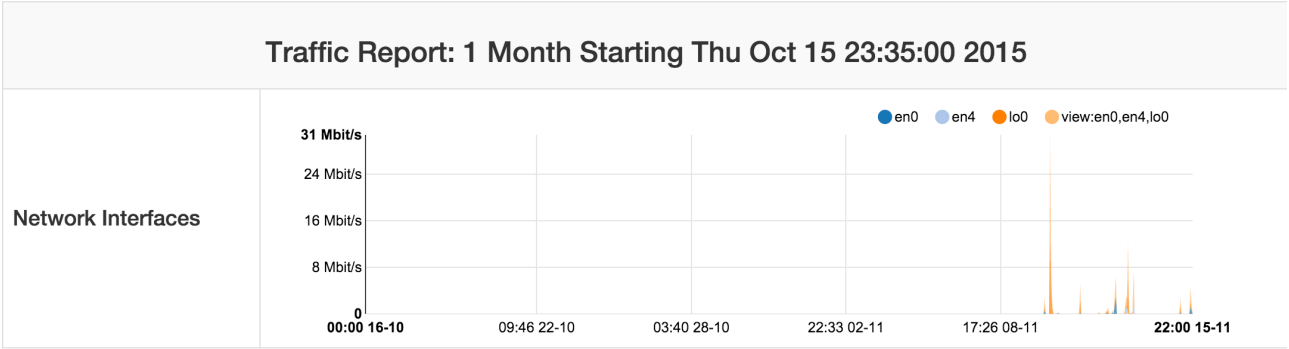


Generated Report - Top Networks and Applications

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.

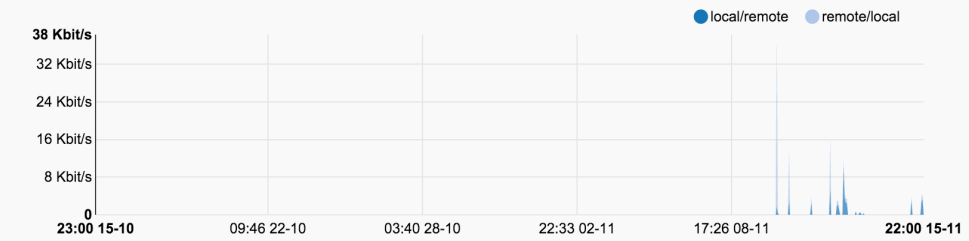


Report - Monitored Network Interfaces Summary

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

Local/Remote

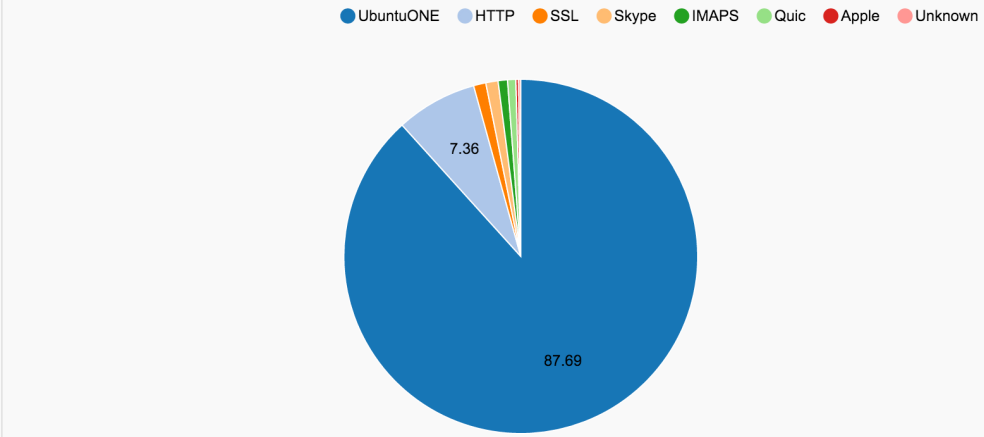


Report - Local to Remote and Remote to Local Traffic

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

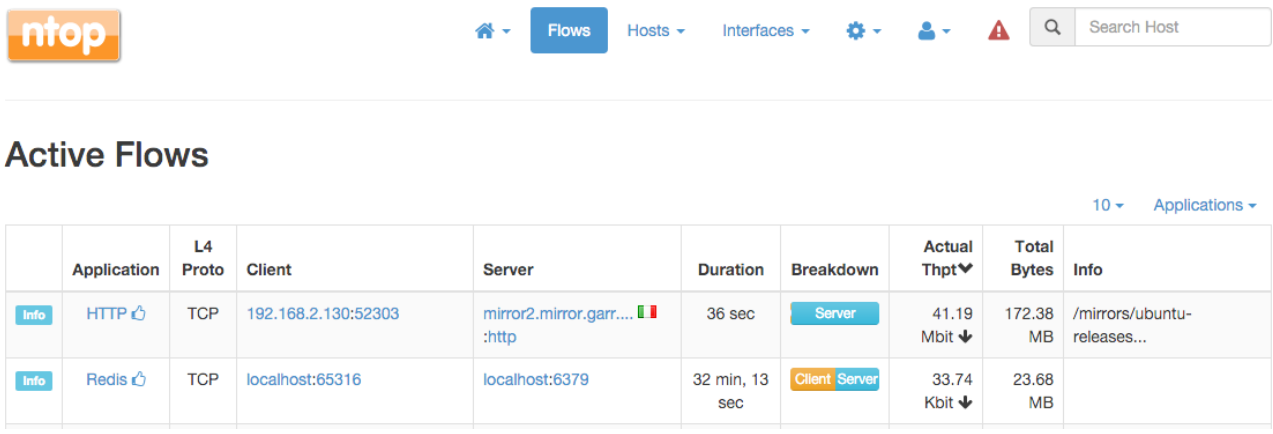
Application Breakdown



Report - Application Breakdown

Flows

The ‘Flows’ entry in the top toolbar can be selected to visualise realtime traffic information on the currently active flows. A flow can be thought of as a logical, bi-directional communication channel between two hosts[1]. Multiple simultaneous flows can exist between the same pair of hosts.



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 NTOP opensource Deep Packet Inspection (DPI) engine named nDPI[2]. 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. An 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 client[3]. 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. An 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 coloured bar gives and indication on the amount of traffic exchanged in each of the two directions. Client to server traffic in shown in orange, while server to client in blue.

Actual Throughput

The throughput is computed periodically (the refresh time is a few seconds)

Total Bytes

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

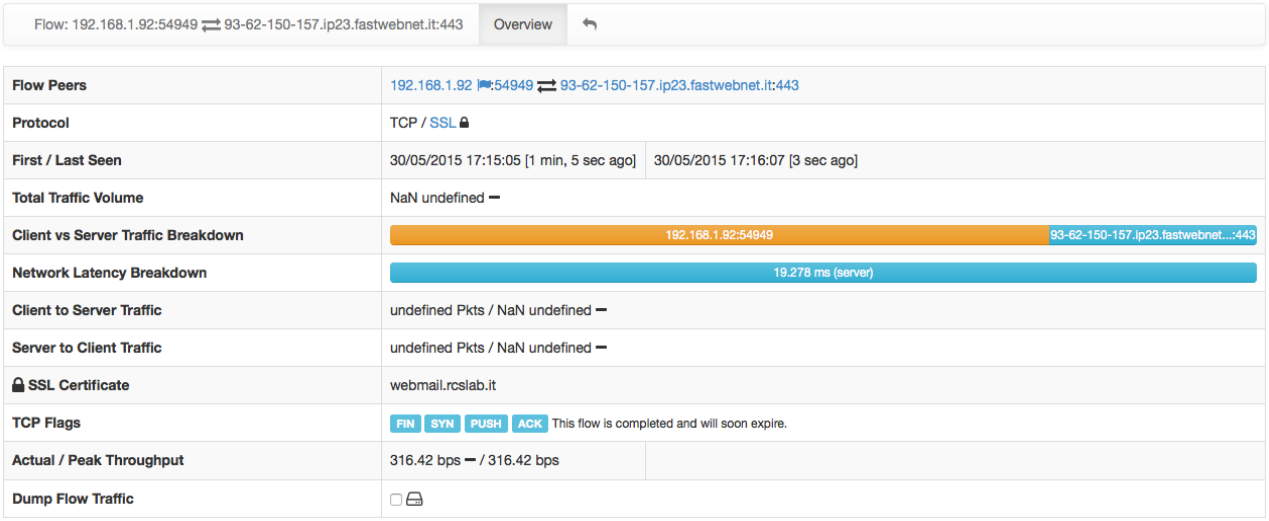
Info

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 Trend[4]
- 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.

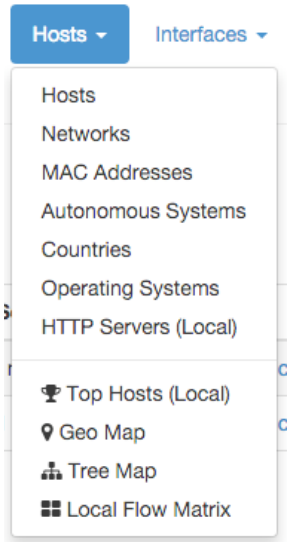


Flow Details Page

[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

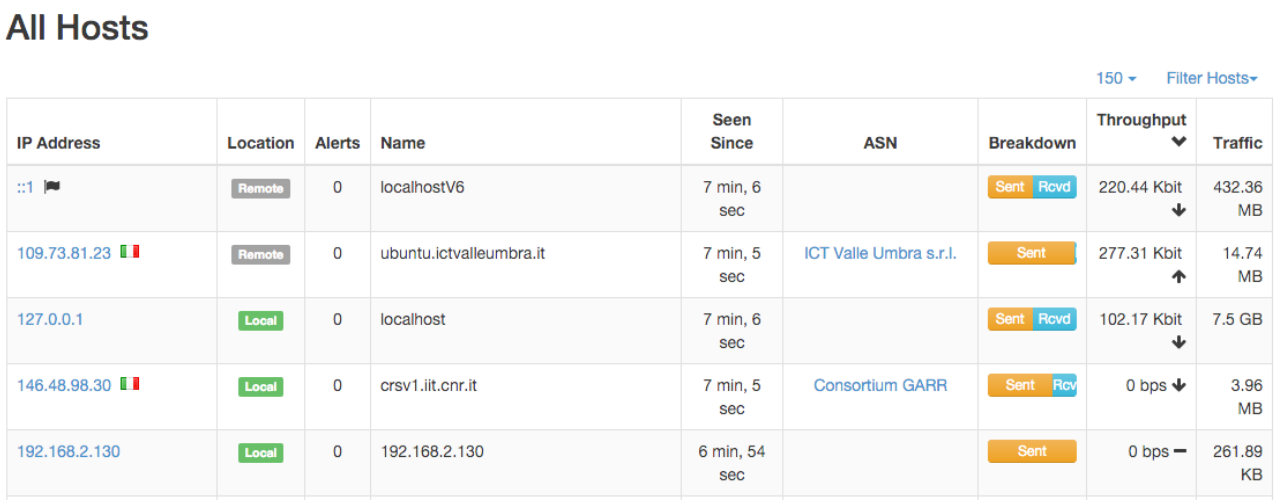
All Hosts

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

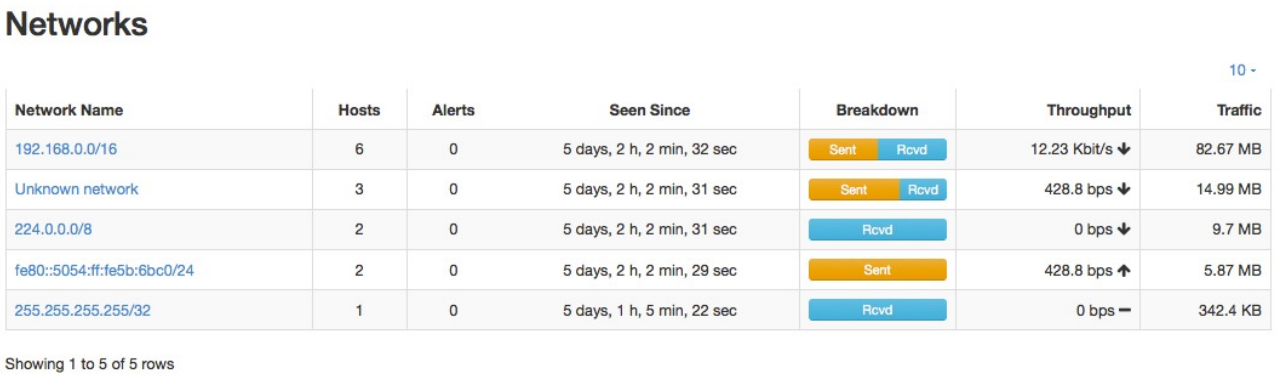


The All Hosts Page

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.

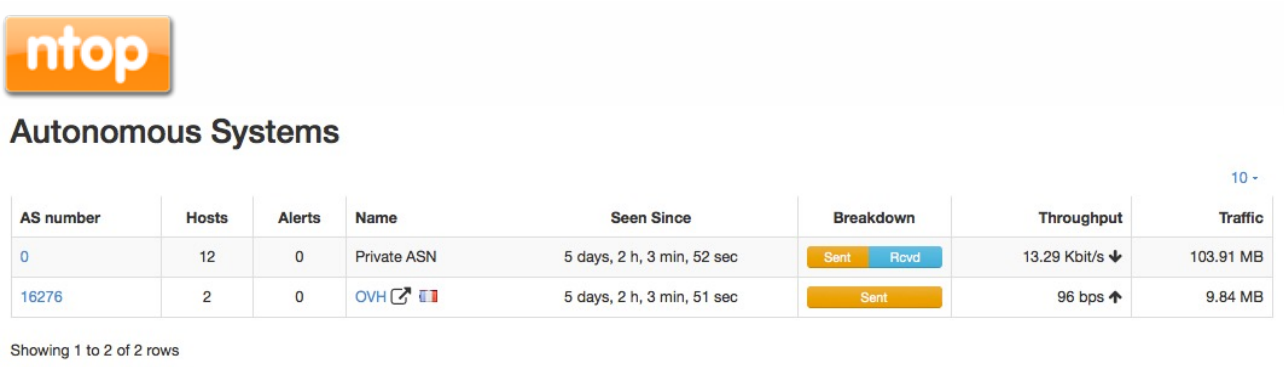


The Networks Summary Page

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

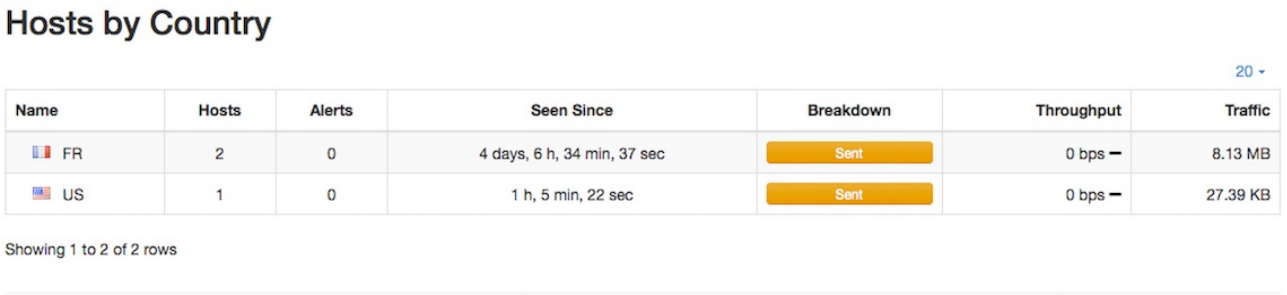
Autonomous Systems shows all autonomous systems discovered by ntopng.



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

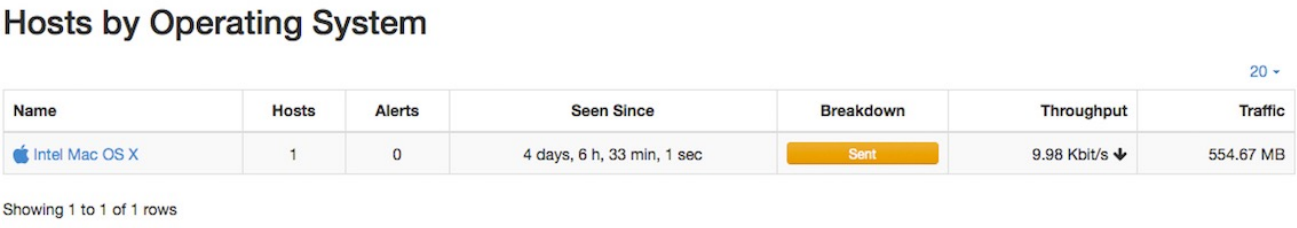
Countries page provides all countries discovered by ntopng. Any country can be clicked to be redirected to a page containing the full list of hosts localised in that country.



The Hosts Countries Summary Page

Operating Systems

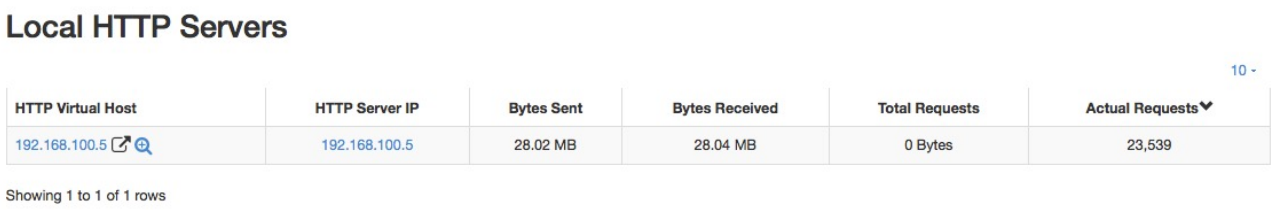
Operating Systems page shows a list of all OS detected by ntopng. OSes can be clicked to see the detailed list of hosts.



The Hosts Operating Systems Summary Page

HTTP Servers (Local)

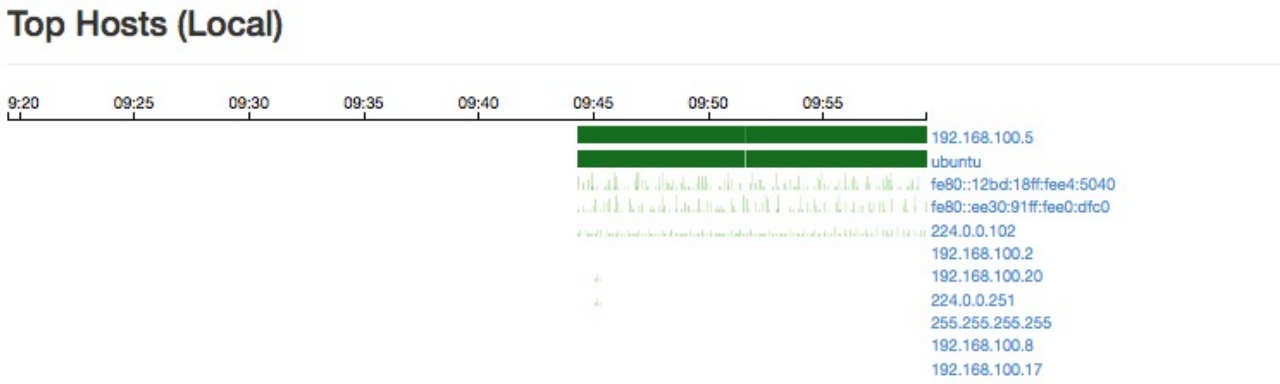
HTTP Servers page lists all local HTTP Servers. Multiple distinct virtual hosts may refer to the same HTTP server IP, which is specified in the second column. Additional information such as bytes sent and received are available for each HTTP virtual host. By clicking on the magnifying lens icon near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



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.



The Top Hosts Summary Page

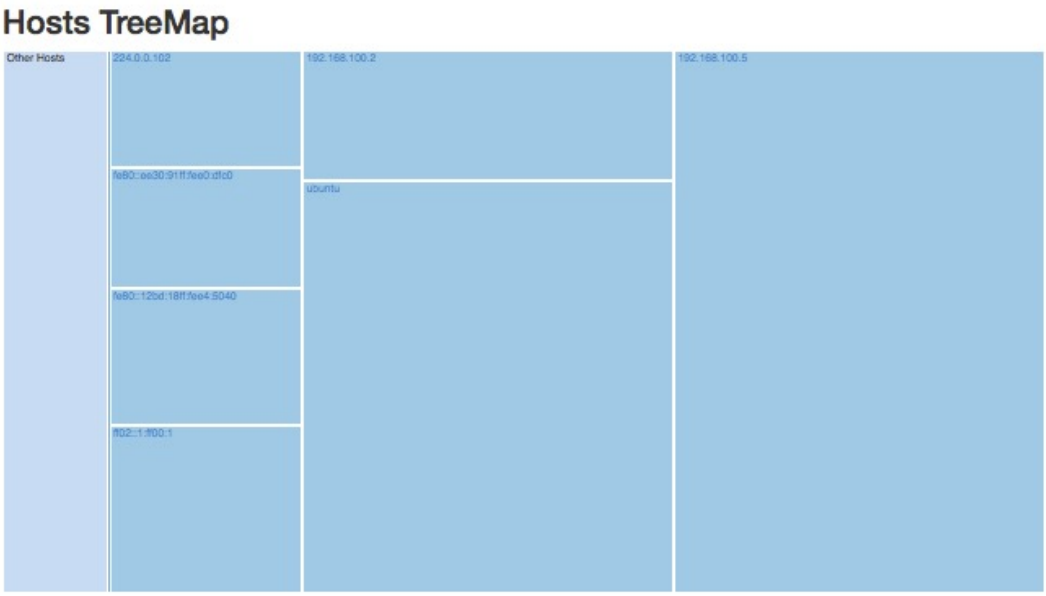
Geo Map

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

The Hosts Geo Map Summary Page

Tree Map

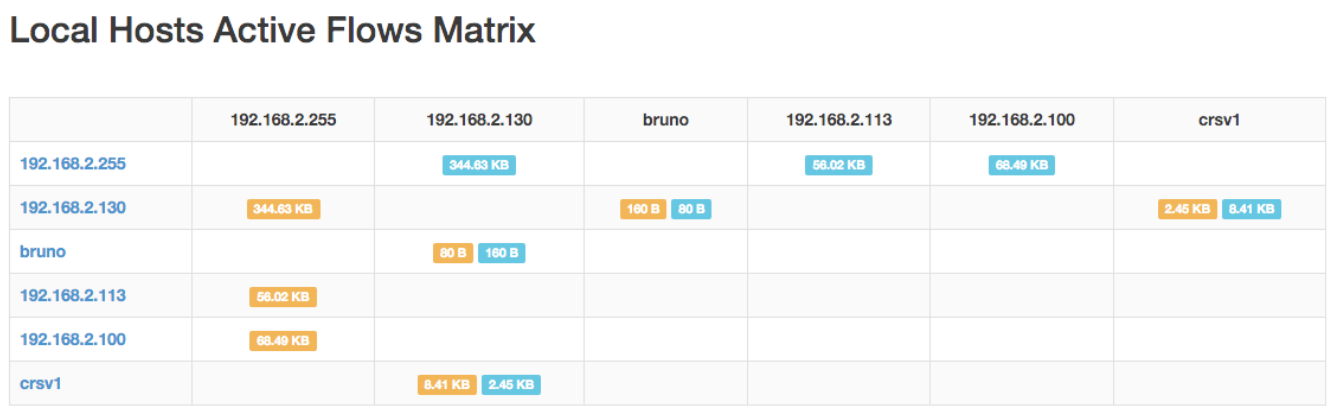
This page provides a tree map of all monitored hosts. By clicking on hosts it is possible to visit the corresponding 'Host Details' page.



The Hosts Tree Map Summary Page

Local Flow Matrix

Local Hosts Active Flows Matrix page visualises 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.



The Active Flows Matrix Page

Host Details

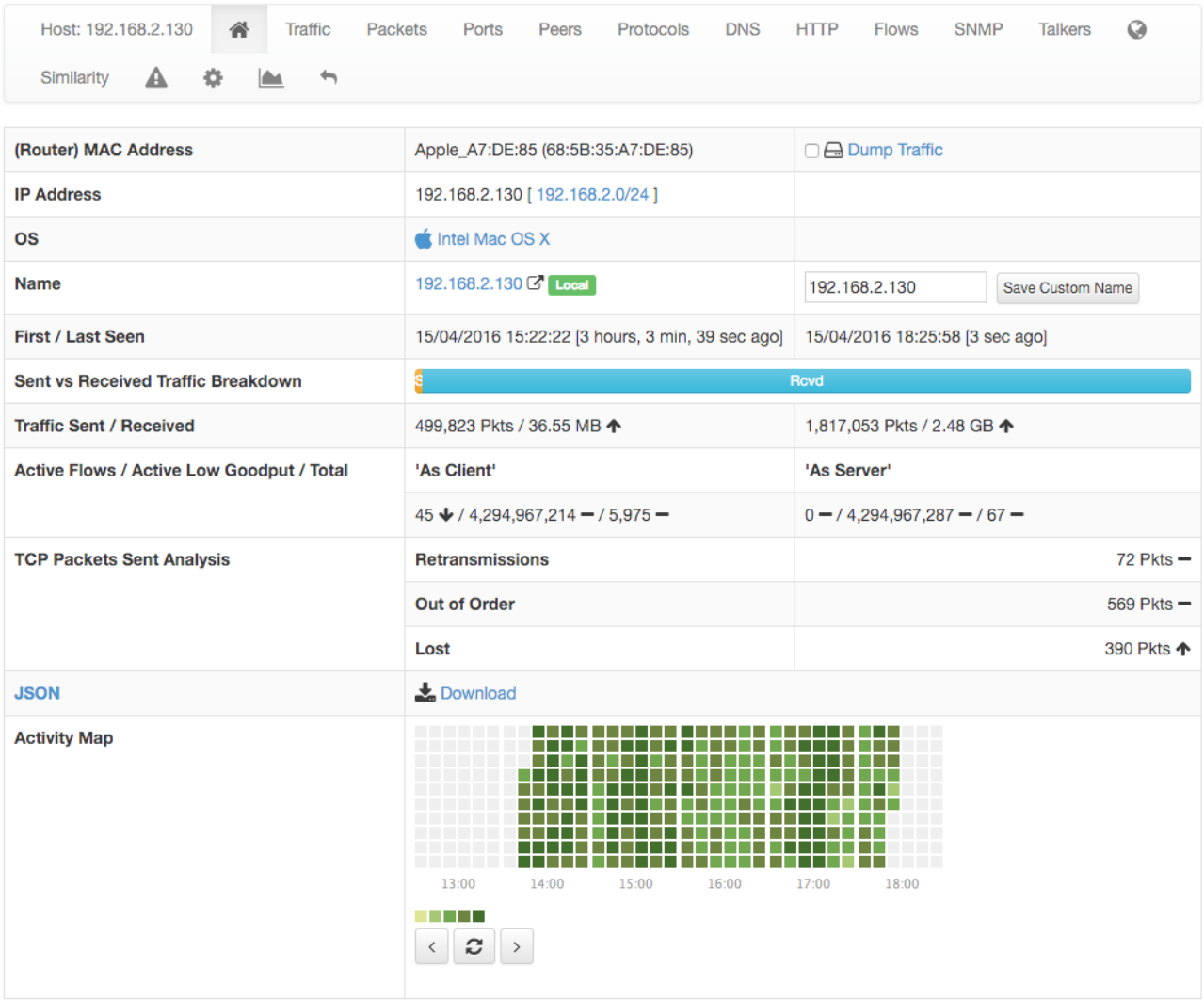
Host Details page is as follows.

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

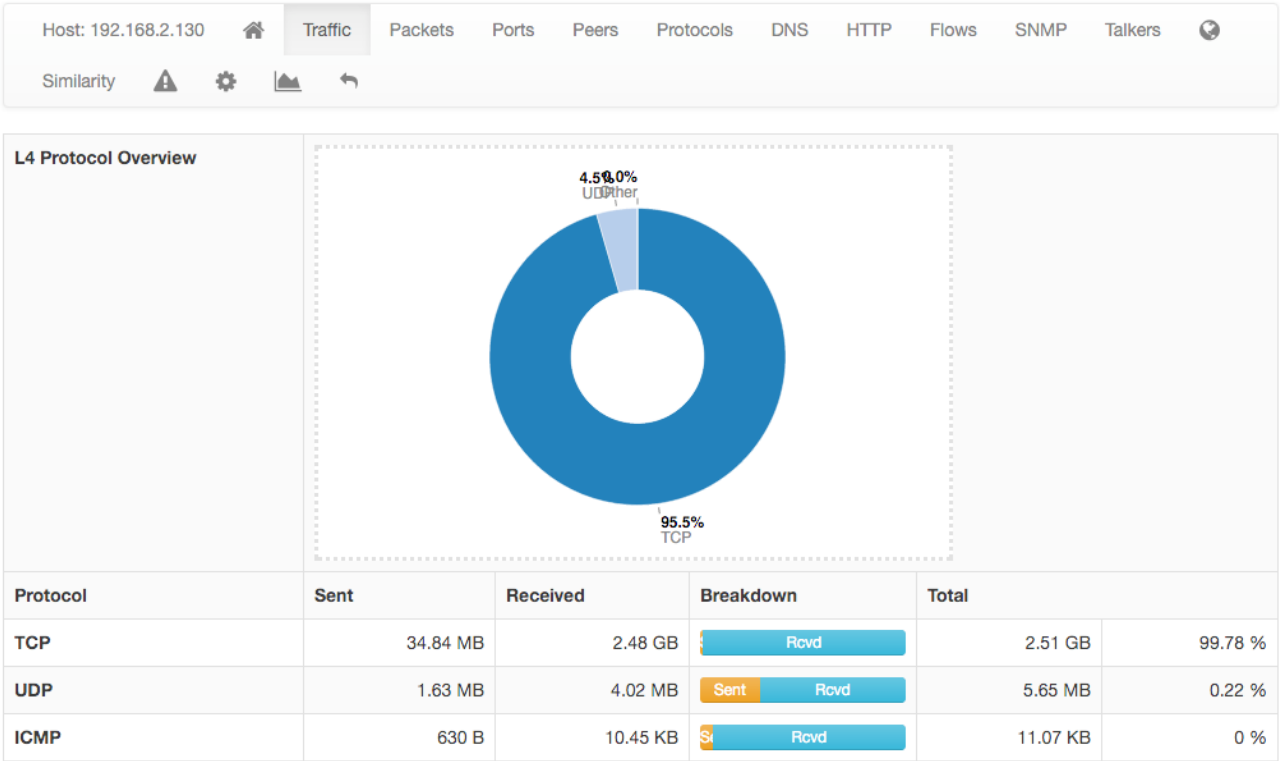
Home is the default view of the Host Details page and provides detailed information including host MAC Address (or the last router MAC address if the host is remote), IP Address (with network mask if detected), a toggle to activate/deactivate alerts for the host, a checkbox to enable packet dump for 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.



The Home View of the Host Details Page

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 the chart.

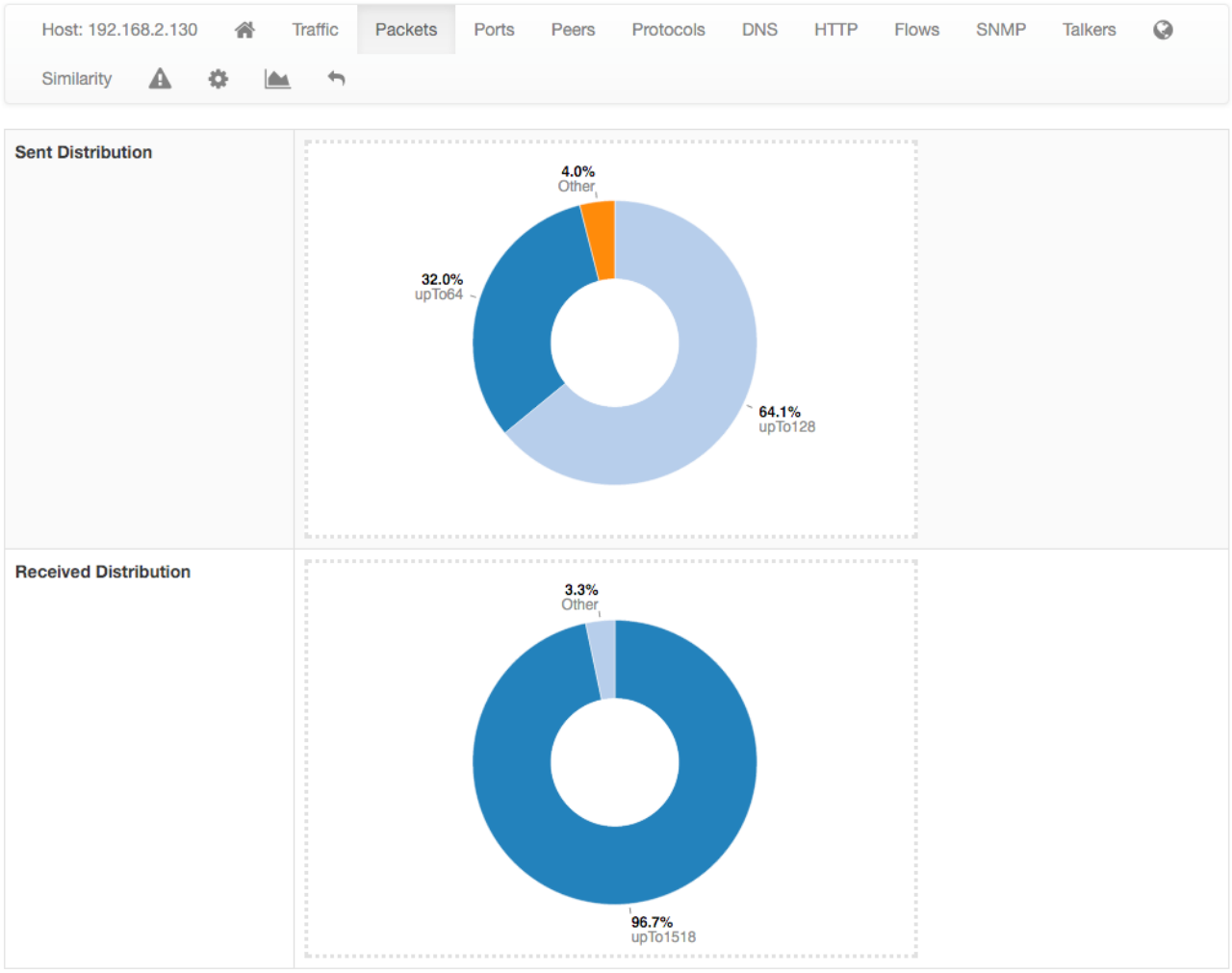


Protocol	Sent	Received	Breakdown	Total	
TCP	34.84 MB	2.48 GB	Rcvd	2.51 GB	99.78 %
UDP	1.63 MB	4.02 MB	Sent Rcvd	5.65 MB	0.22 %
ICMP	630 B	10.45 KB	Rcvd	11.07 KB	0 %

The Traffic View of the Host Details Page

Packets

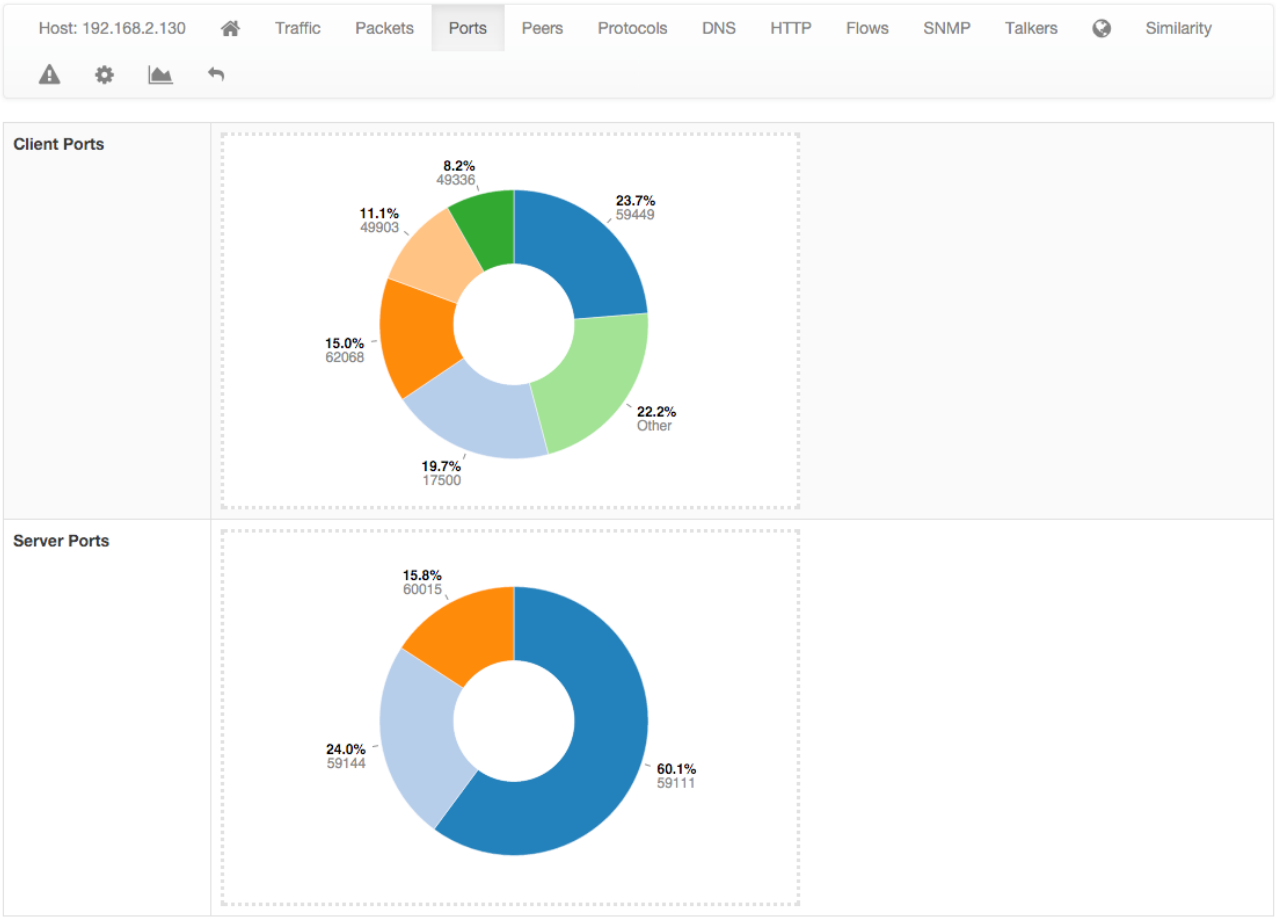
Packets page provides pie charts with packet size distribution, both for sent and received packets.



The Packets View of the Host Details

Ports

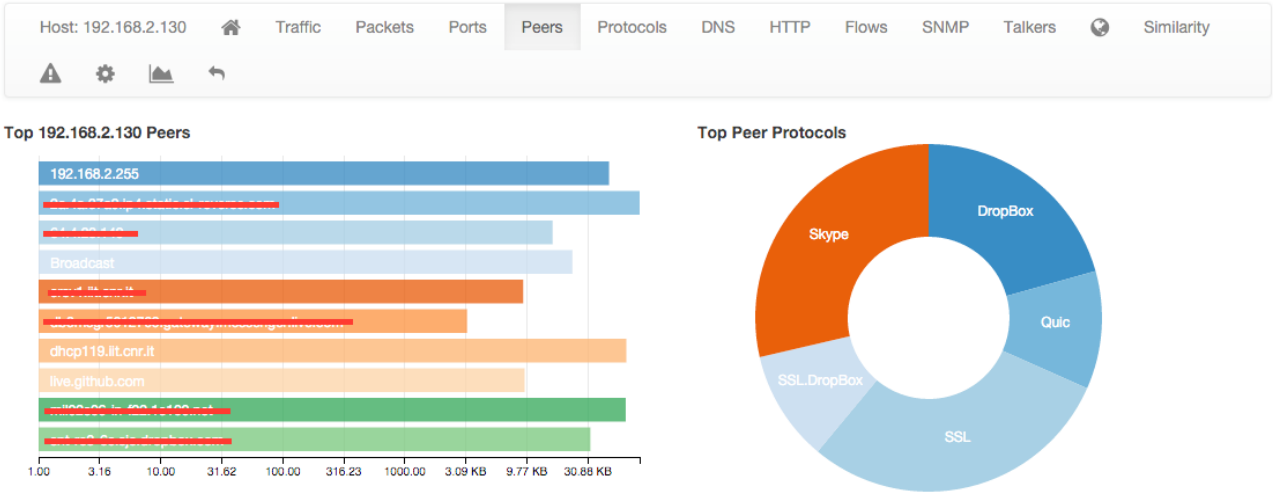
Ports page provides pie charts with traffic statistics grouped by port. A chart is available for client ports and another one is available for server ports.



The Ports View of the Host Details Page

Peers

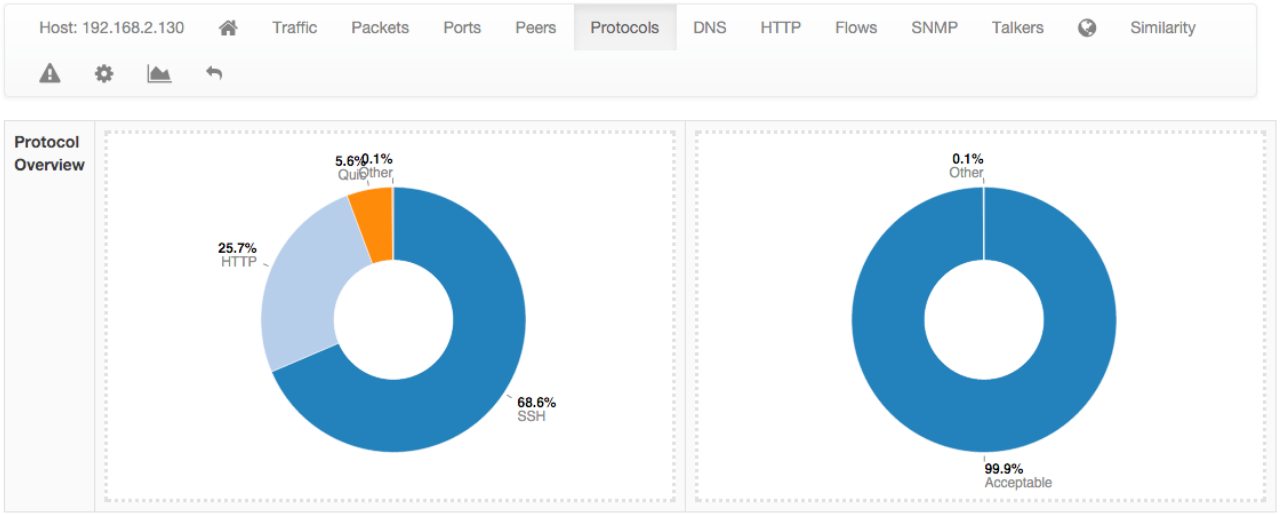
Peers page presents a graphical overview of top contacted peers and top protocols used. In the following screenshot some hosts are struck-through intentionally for privacy reasons. A table with top application per peer is shown below the graphical overview. Every information is clickable to allow the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

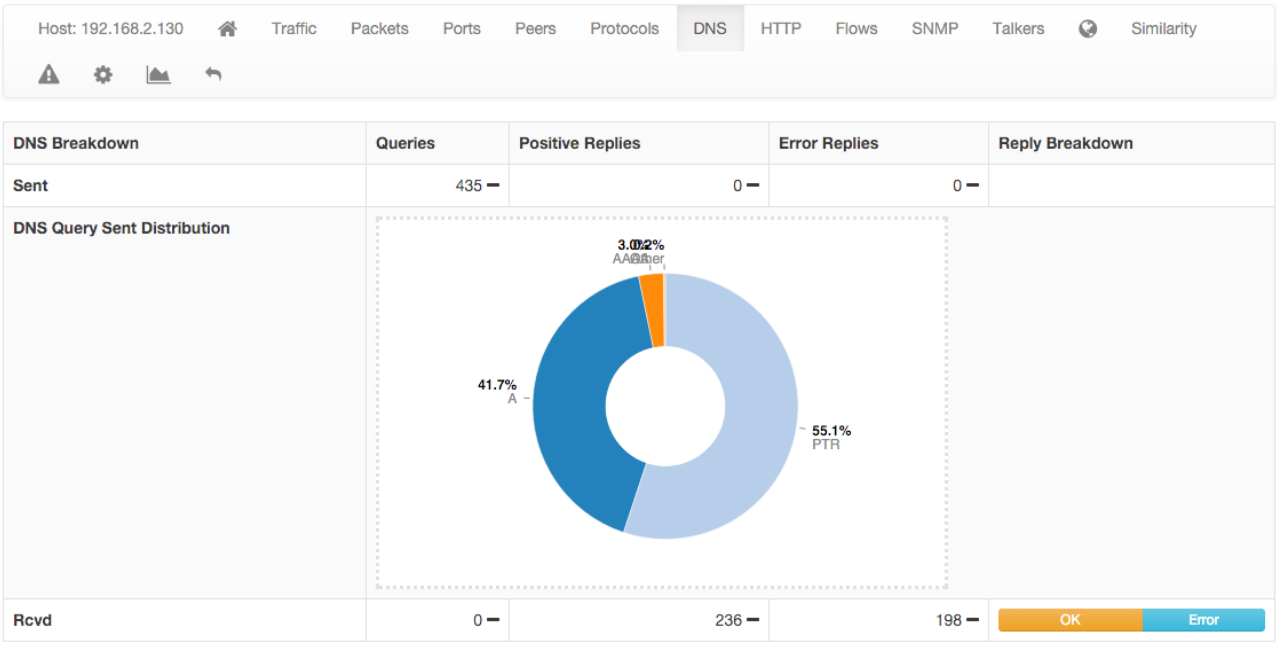


Application Protocol	Sent	Received	Breakdown	Total	
Total	2.07 GB	963.07 MB	Sent Rcvd		3.02 GB
Apple	7.21 KB	22.34 KB	Sent Rcvd	29.55 KB	0 %
AppleiCloud	18.78 KB	39.08 KB	Sent Rcvd	57.86 KB	0 %
AppleiTunes	16.56 KB	56.41 KB	Sent Rcvd	72.97 KB	0 %
DNS	22.32 KB	49.17 KB	Sent Rcvd	71.48 KB	0 %
DropBox	202.73 KB	62.44 KB	Sent Rcvd	265.17 KB	0.01 %
Facebook	2.55 KB	16.87 KB	Sent Rcvd	19.41 KB	0 %
GMail	65.31 KB	91.83 KB	Sent Rcvd	157.14 KB	0 %
Google	150 KB	240.01 KB	Sent Rcvd	390 KB	0.01 %
HTTP	7.78 MB	786.52 MB	Rcvd	794.29 MB	25.72 %
ICMP	644 B	3.47 KB	Sent Rcvd	4.1 KB	0 %

The Protocols View of the Host Details Page

DNS

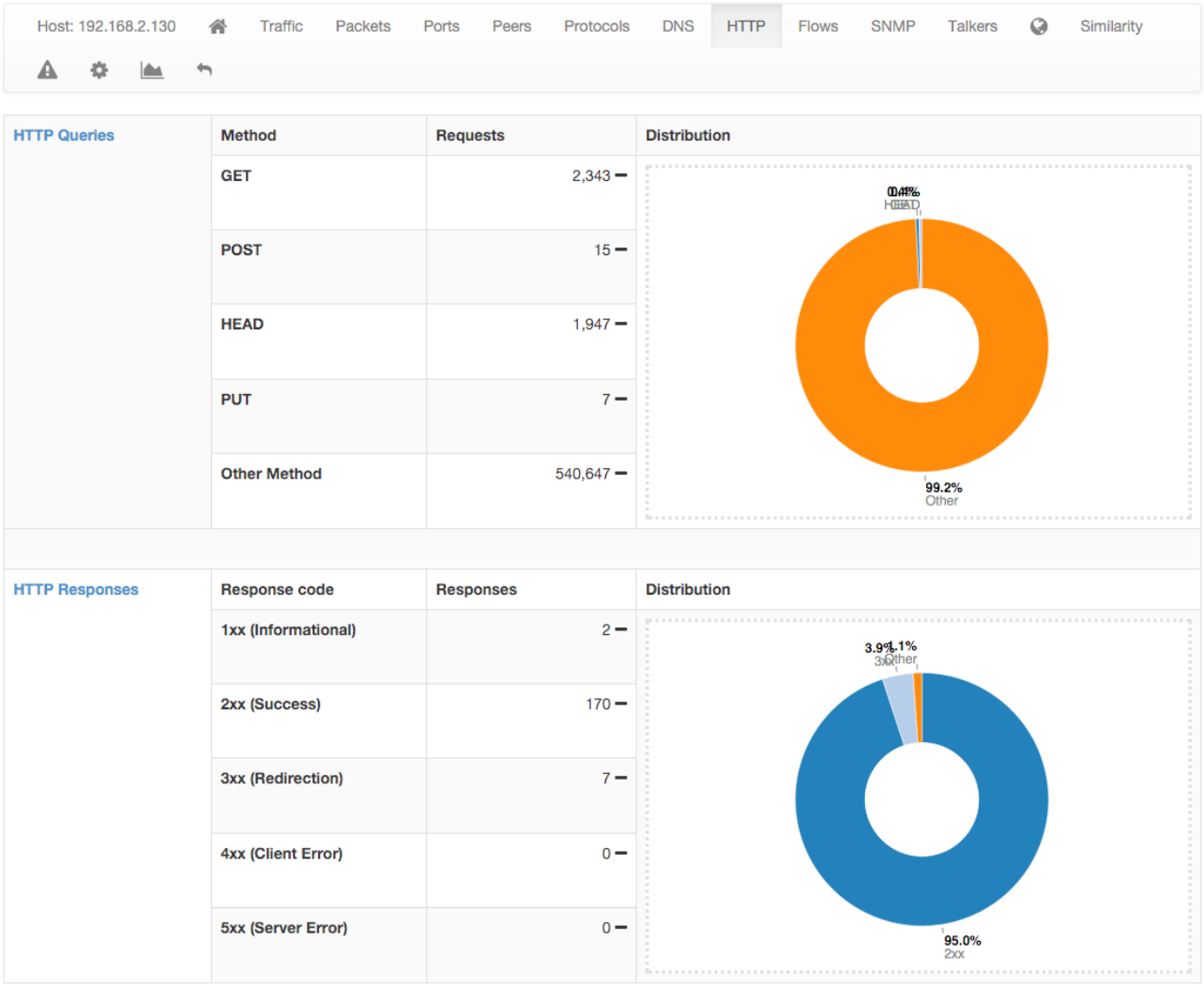
The chart and the table displayed on this page report DNS statistics, such as the number of queries, their type (e.g., A, AAAA, PTR, and so on), and possible errors.



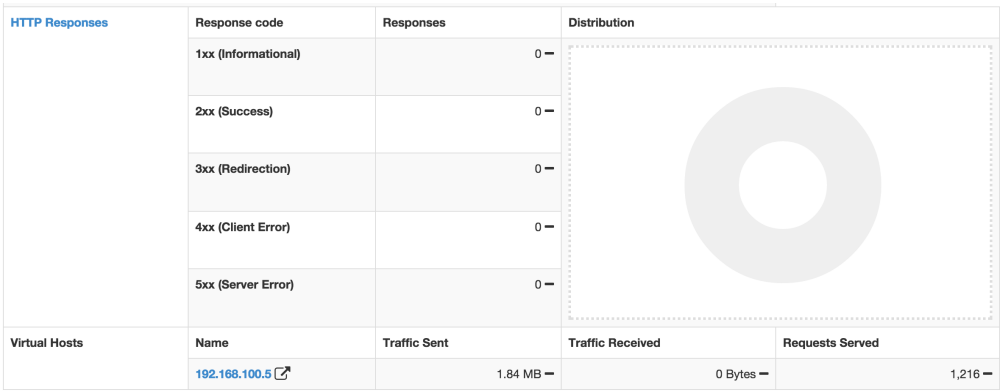
The DNS View of the Host Details Page

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.



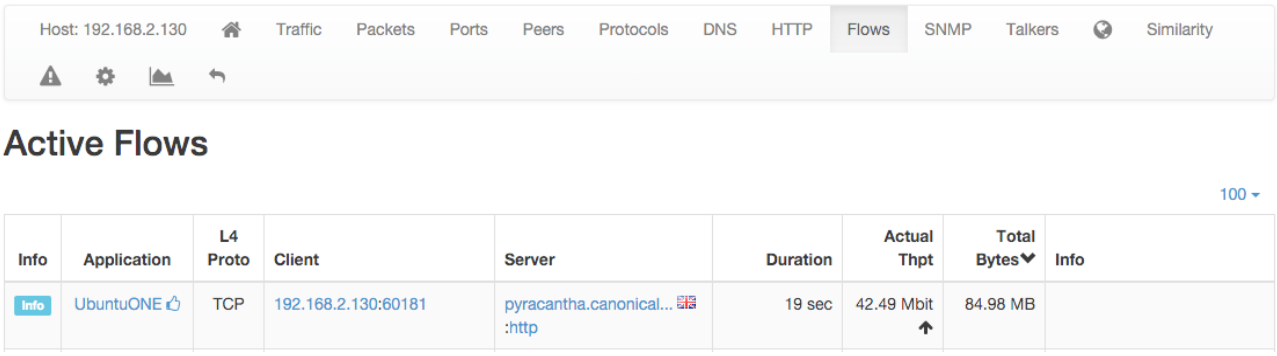
The HTTP View of the Host Details Page



The HTTP View of the Host Details Page with Virtual Hosts

Flows

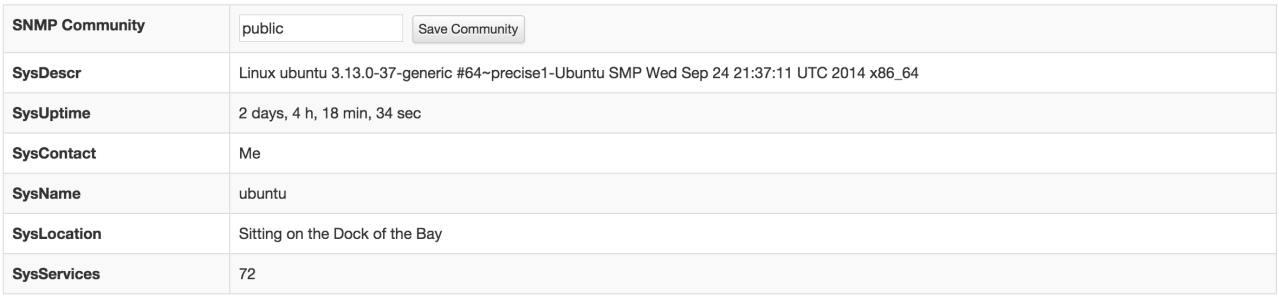
Flows page lists all active flows that have the selected host as an endpoint. A section of this manual discuss in greater detail the statistics shown for flows.



The Flows View of the Host Details Page

SMNP

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



The SMNP View of the Host Details Page

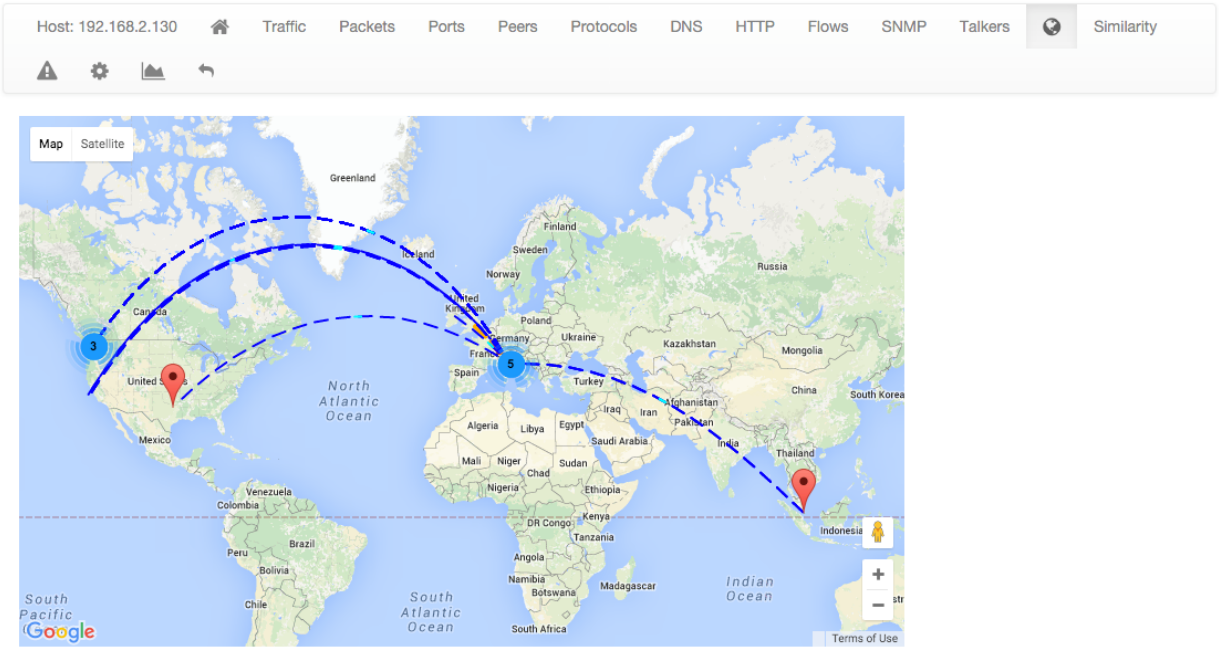
Talkers

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

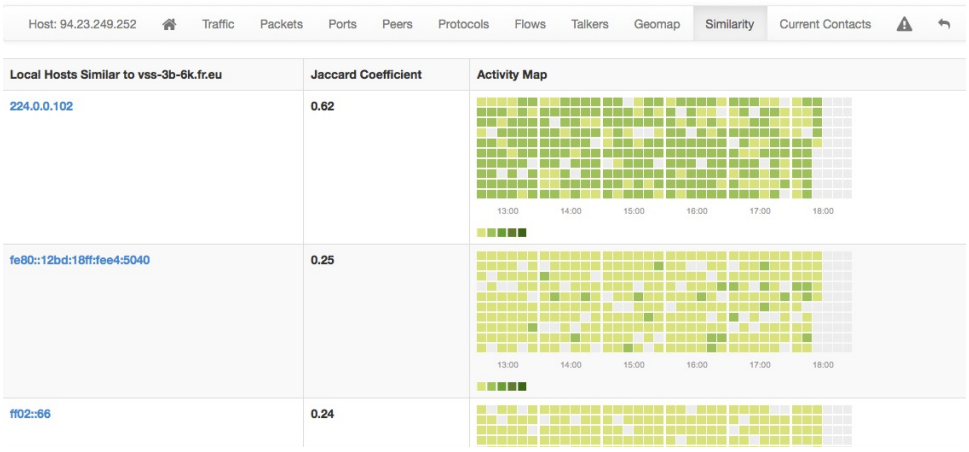
Geography page provides an interactive map that shows the selected hosts, its flows, and its peers.

Similarity



The Geography View of the Host Details Page

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 Coefficient[5]

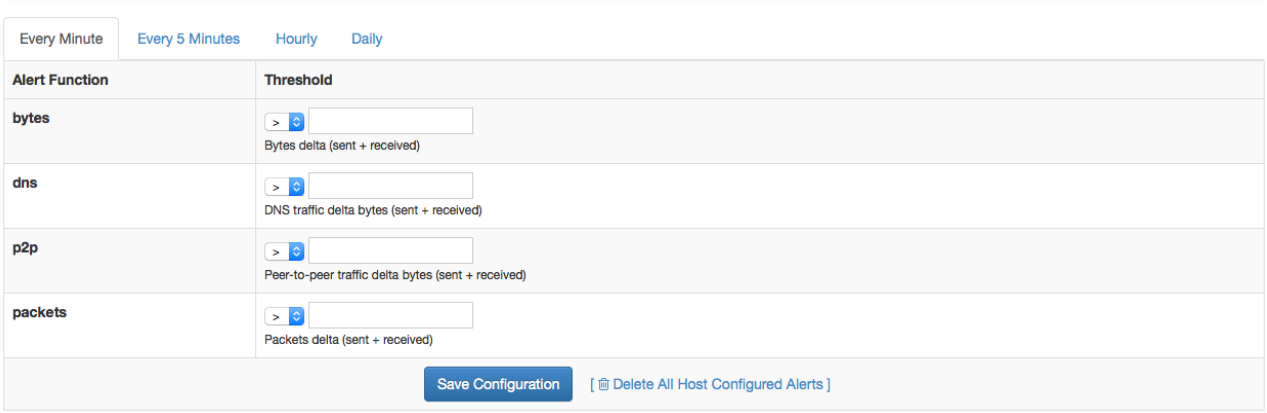


The Similarity View of the Host Details Page

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

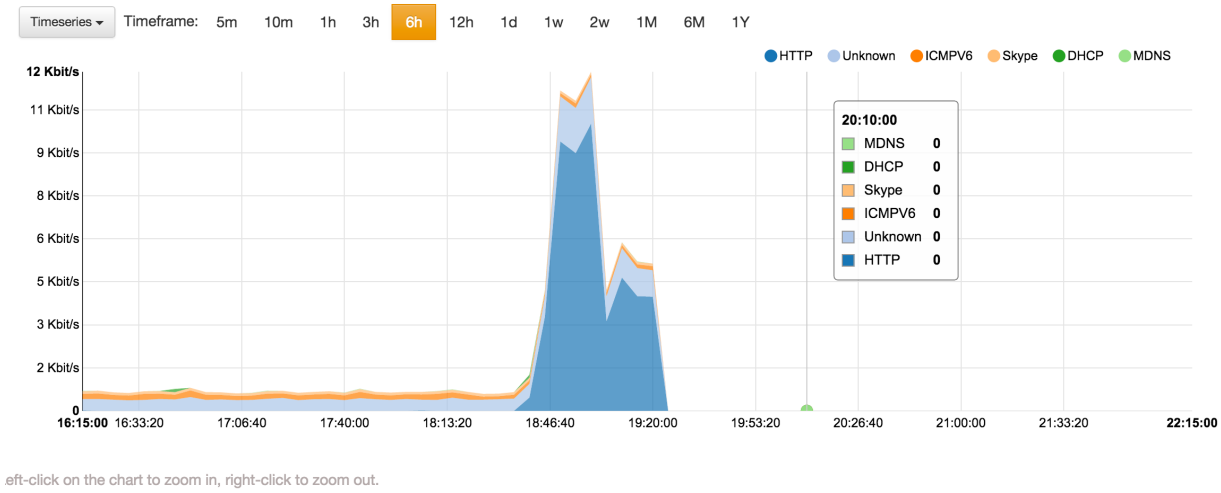
Alerts Configuration

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.

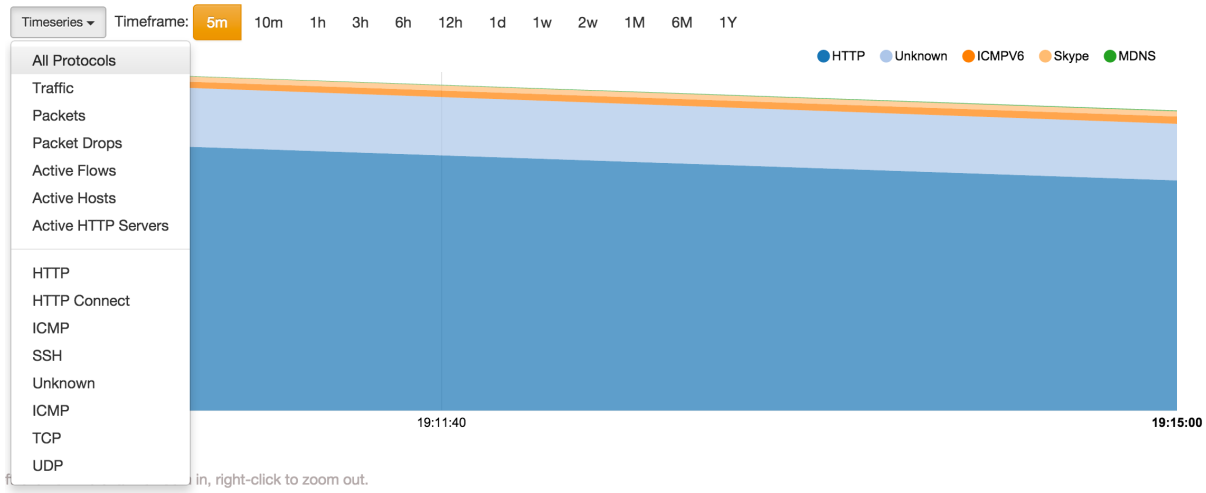


Statistics

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).



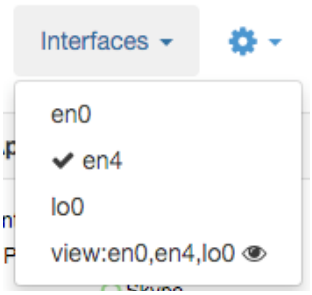
The Statistics View of the Host Details Page



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

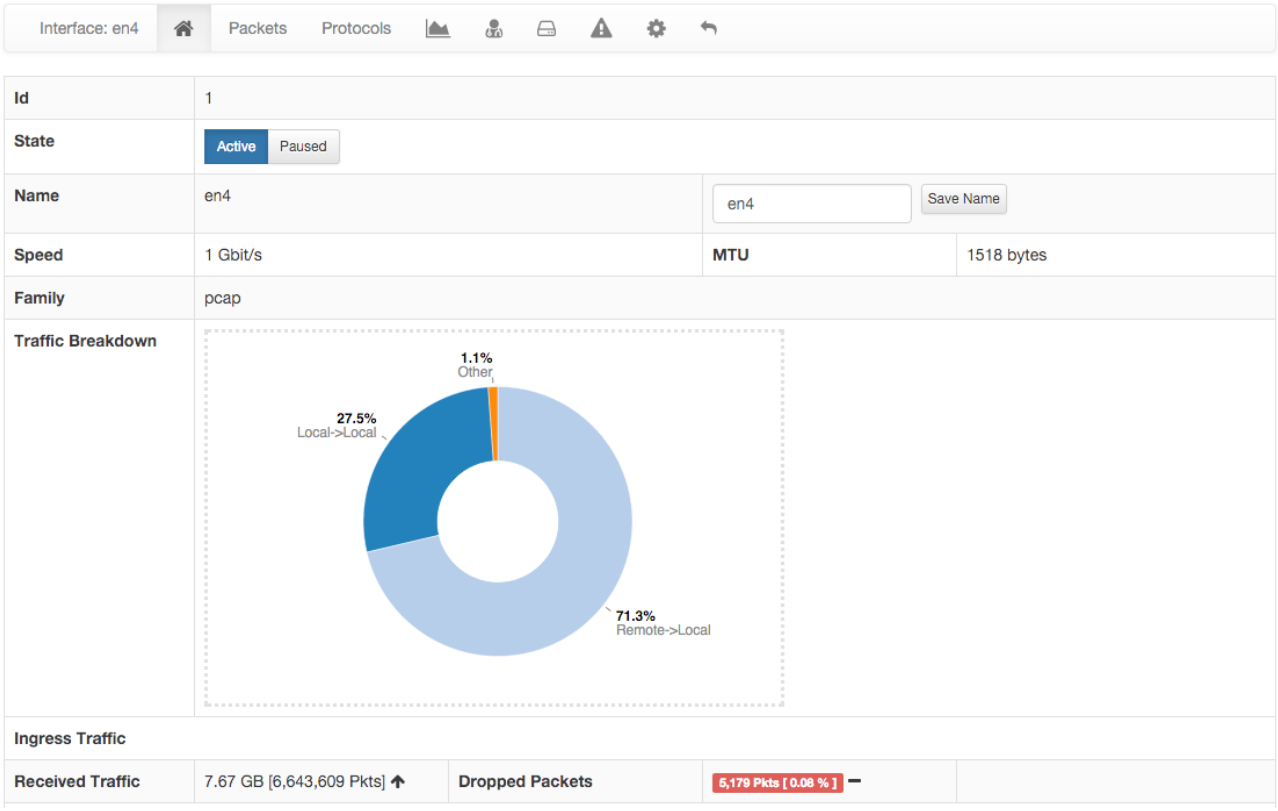
Interfaces

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.



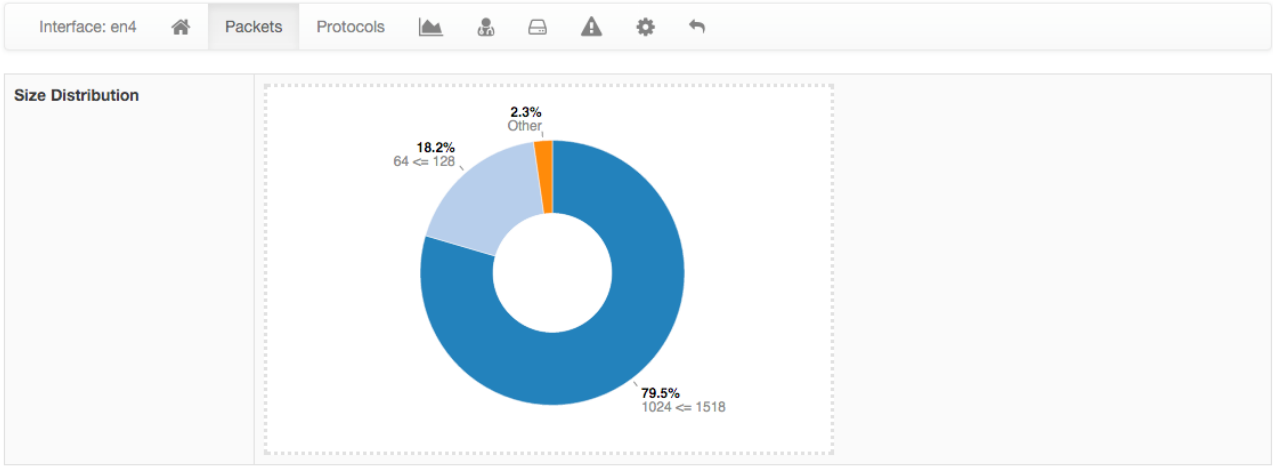
The Home View of the Interface Details Page

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 customise 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

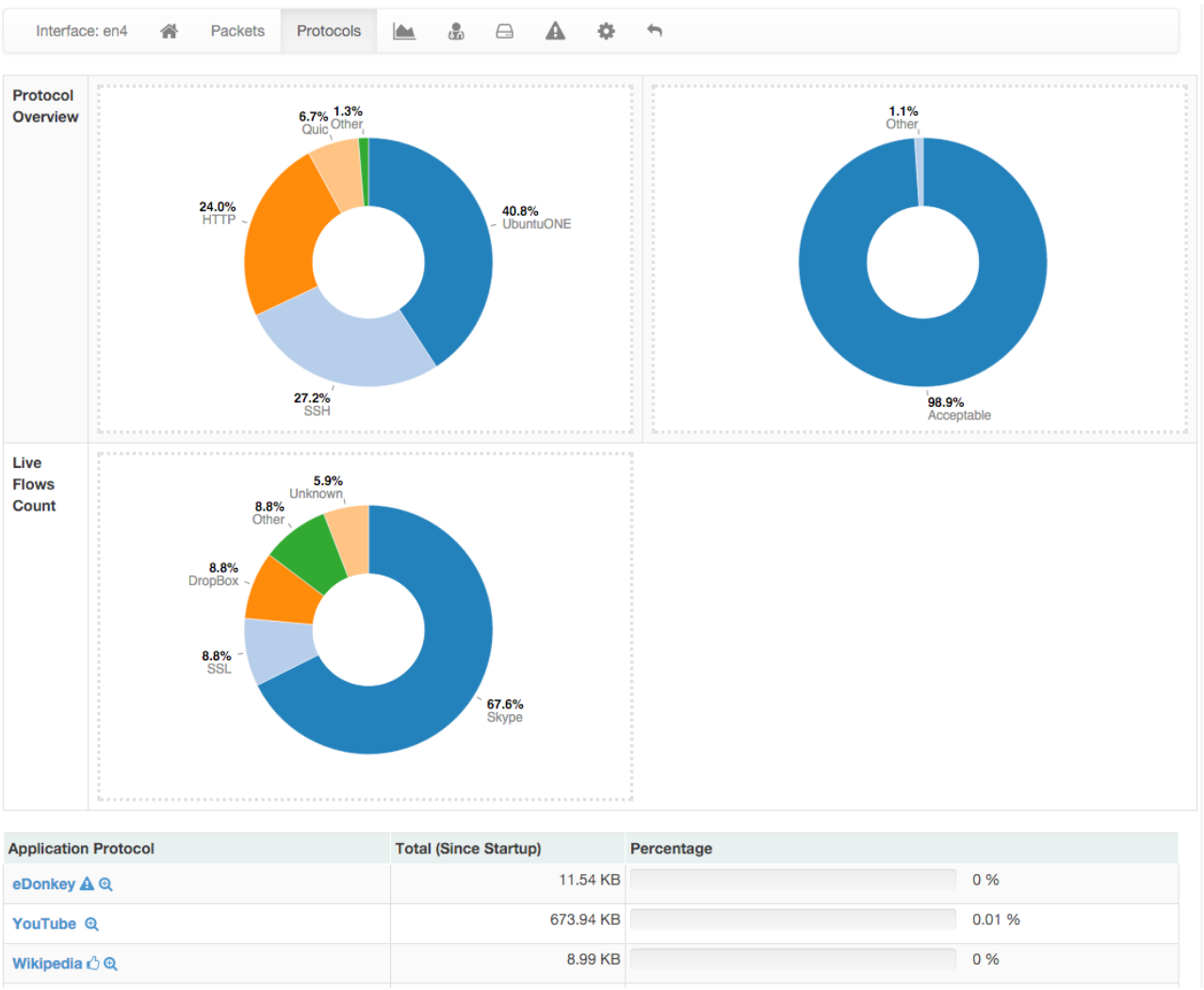
Packets page shows a pie chart of packets size distribution.



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.

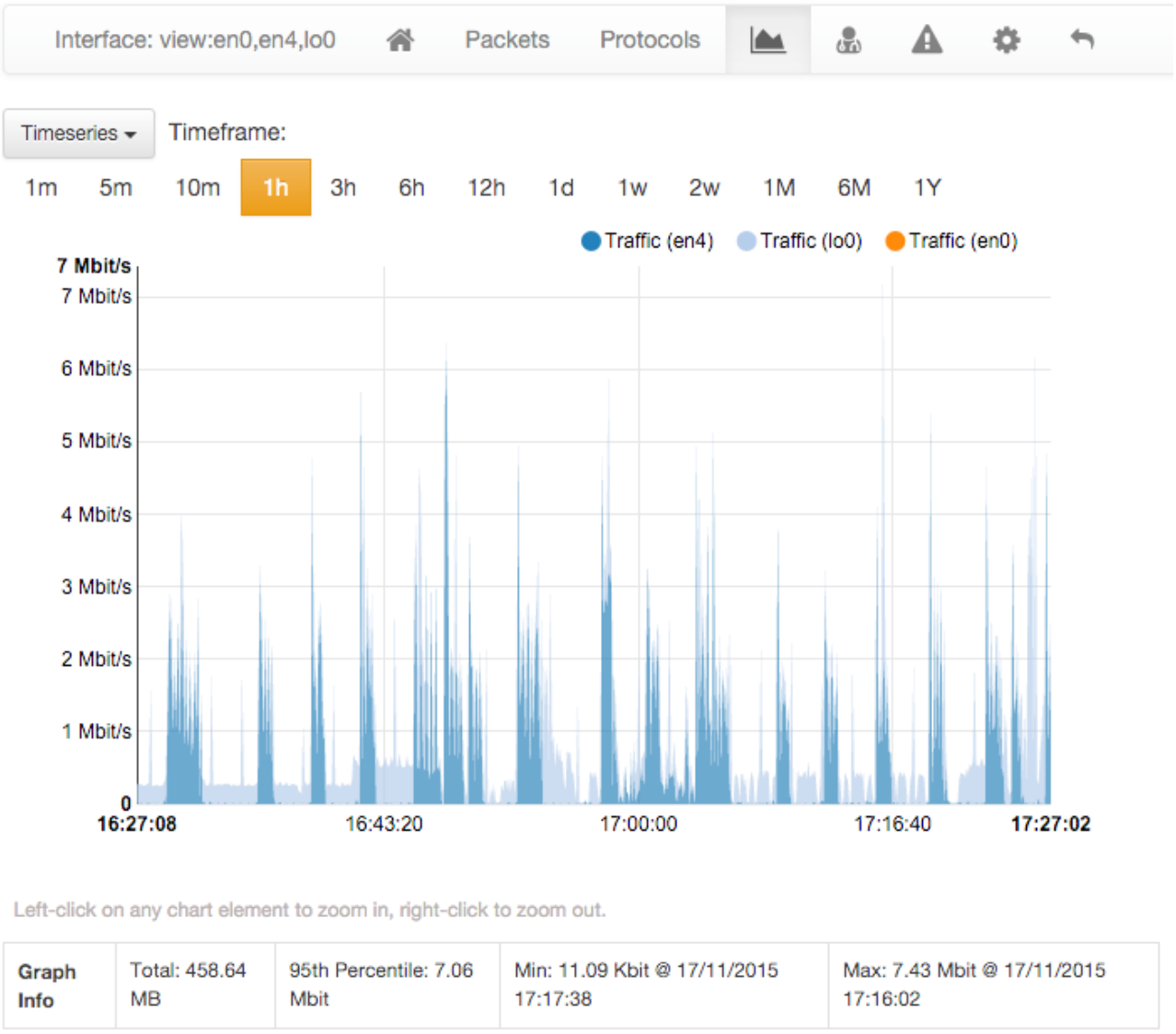


The Protocols View of the Interface Details Page

In the two top pie charts ntopng shows the application distribution and its categorisation. The bottom pie chart shows nDPI-detected applications for currently active flows. All labels are clickable and point to detailed statistics pages. Belo 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

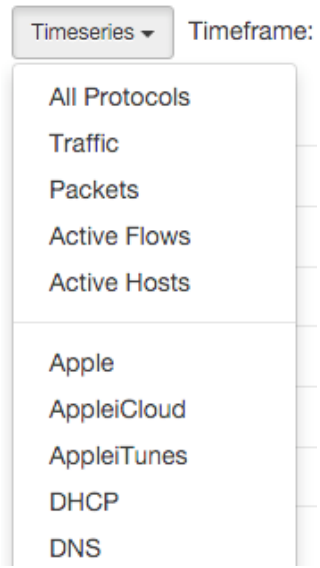
Statistics page provides historical traffic statistics for the selected interface. The user can choose to filter statistics on a protocol basis and display data in several formats (e.g., bytes, packets, flows, and so on). In the Professional Version of ntopng, traffic for interface views in shown as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



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

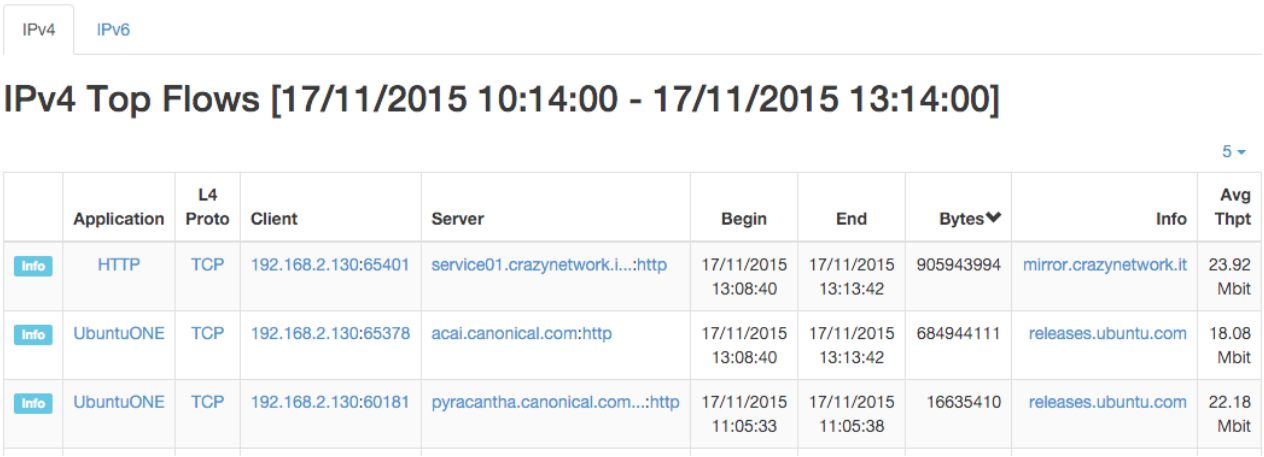
The time series span can be adjusted by selecting values from 5 minutes up to 1 year. Moreover, drill-down is possible by clicking on the time series itself. Every click zooms the chart in, centering the time series around the clicked point.

Moreover, time series shown can be chosen via the dropdown menu labelled ‘Time series’. For example, it is possible to visualise 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.



	Application	L4 Proto	Client	Server	Begin	End	Bytes	Info	Avg Thpt
Info	HTTP	TCP	192.168.2.130:65401	service01.crazynetwork.i...: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

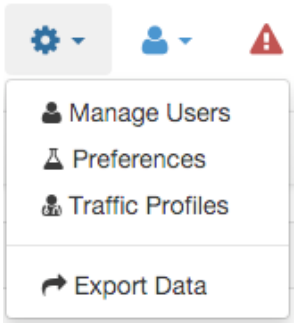
Traffic Profiles (Professional Version)

See later in this manual for more information.

Packet Dump

This page allows you to save to disk selected packets that match various

Settings

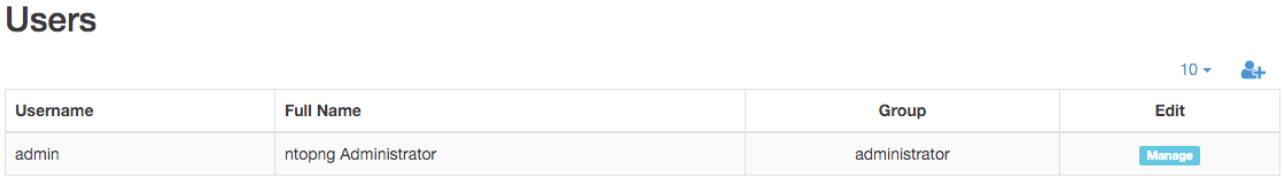


The Dropdown Settings Menu in the Top Toolbar

The Runtime settings can be configured using the dropdown gear menu in the top toolbar.

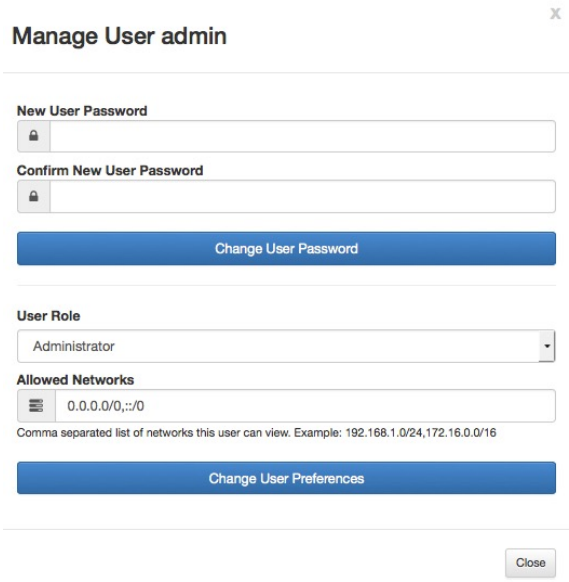
Manage Users

Manage Users menu gives access to ntopng users administration. Ntopng is a multi-user system that handles multiple simultaneous active sessions. Ntopng users can have the role of Administrators or standard users.



The Manage Users Settings Page

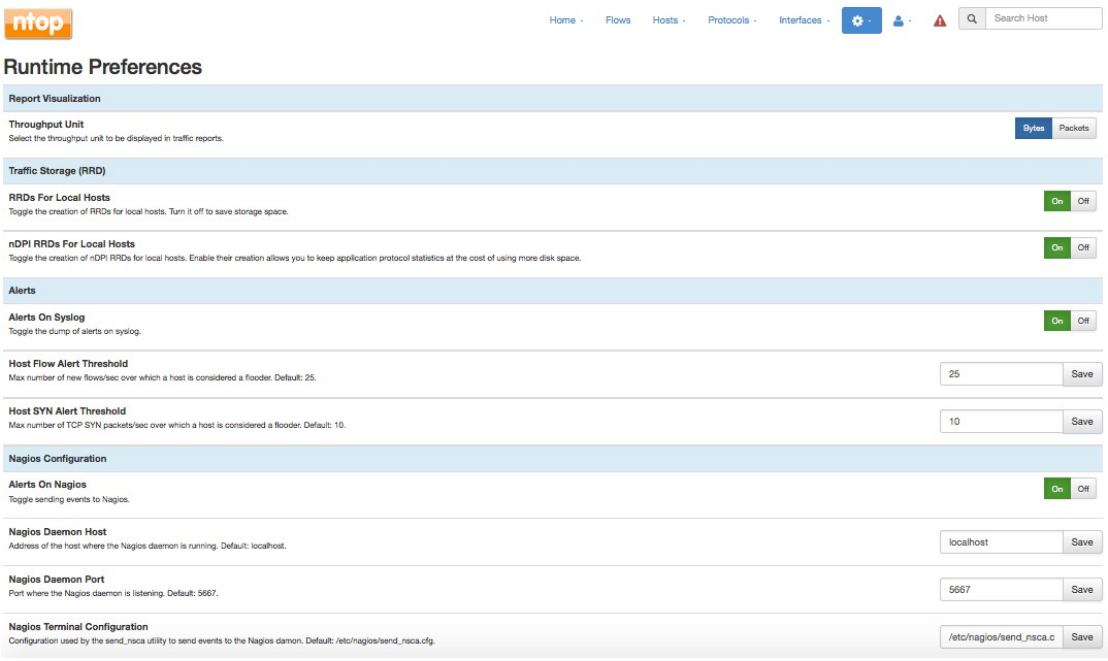
Password and other preferences such as role and allowed networks can be changed my clicking on button Manage, which causes a new window to pop out



The Manage User Pop Up

Preferences

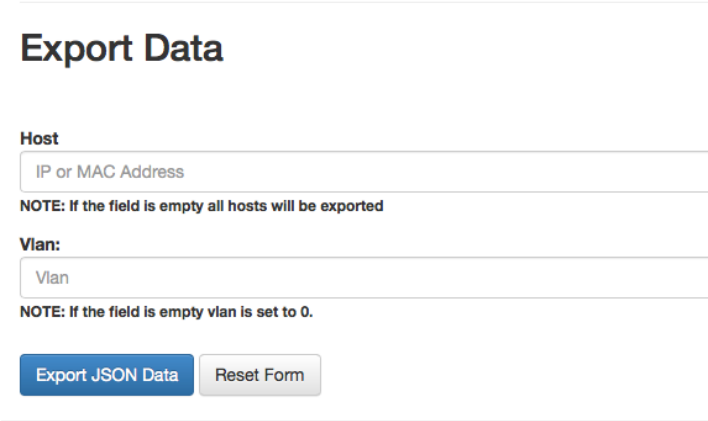
Preferences menu entry enables the user to change runtime configurations. A thorough help is reported below every preference directly into ntopng web GUI.



The Runtime Preferences Settings Page

Export Data

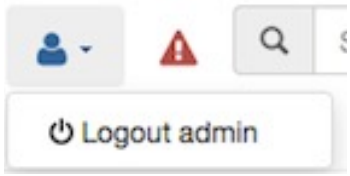
Ntopng is able to export monitored hosts information. It allows to export data in JSON format giving the user the ability to include ntopng information in a user created GUI.



Export Data Page

Administration

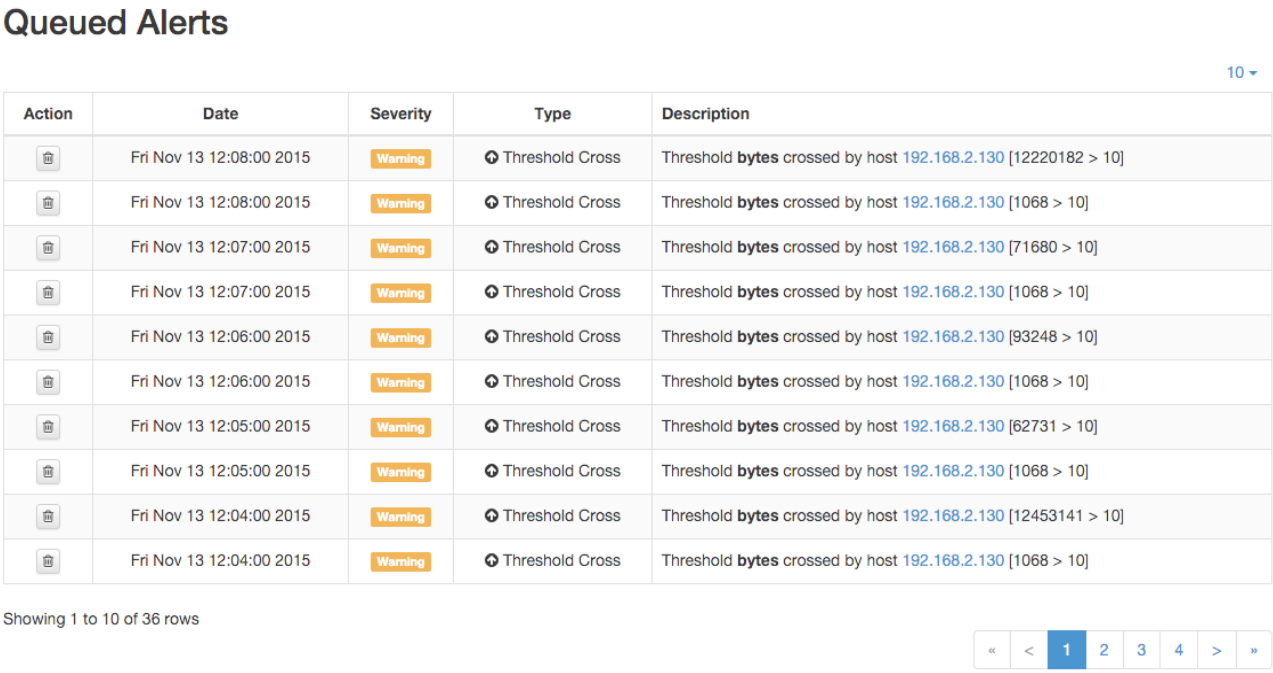
This menu entry contains a logout button to disconnect the used from the ntopng GUI.



The Administration Menu

Alerts

The Alerts Menu opens a page with the list of alerts that was fired. This icon is hidden if no alerts was triggered or after purge operation. Each row in the Alerts page presents an alert detected by ntopng with information such as Date, Severity, Type and Description.



The Alerts Page

Host Search

The Search Box

This box allows to display all information about a specific host. Dynamic auto completion enables users to check whether the searched host appears in the list while typing.

Advanced ntopng Features

Advanced ntopng features such as logical interface aggregation and bridging are described in this section.

Physical Interfaces Aggregation: Interface Views

Ntopng can aggregate two or more physical interfaces into logical units, the so called *Interface Views*. Interface views are seen and treated in the web GUI as if they were real interfaces. In the background, ntopng collects statistics and traffic for every physical interface underlying an interface view, and reduce these multi-source stream of information into a single logical aggregate.

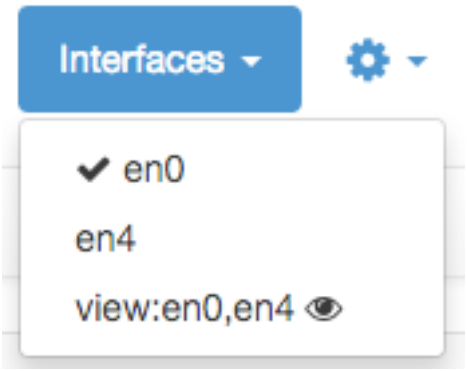
Interface views are specified via command line (or configuration file), using the same *-i* modified that is used for physical interfaces. An extra *view:* string must be added right after the -i modifier to tell ntopng that it is going to read a view. Physical interfaces must be indicated in a comma separated list that follows the *view:* string.

For example an interface view that merges physical interfaces *en0* and *en4* can be created using the following syntax

```
ntopng -i en0 -i en4 -i view:en0,en4
```

Interfaces that are part of a view must also be specified separately as physical interfaces. This means that you cannot omit the -i en0 -i en4 from the example above.

Upon successful startup, ntopng shows, in the top toolbar 'Interfaces' menu, the interface view together with other physical interfaces. An eye is show next to each view, which can be clicked and selected as if it was a physical interface.



The Interfaces Dropdown Menu in the Top Toolbar

Traffic Profiles

Traffic profiles allow the user to define logical aggregations of traffic. Examples of logical aggregates of traffic include 'TCP traffic flowing from local network 192.160.1.0/24 to host 10.0.0.1', 'Facebook traffic originating at host 192.168.10.20', and so on.

Traffic Profiles are a feature that is only available in the Professional Version of ntopng.

Profiles can be set and configured via the dropdown menu in the top toolbar.

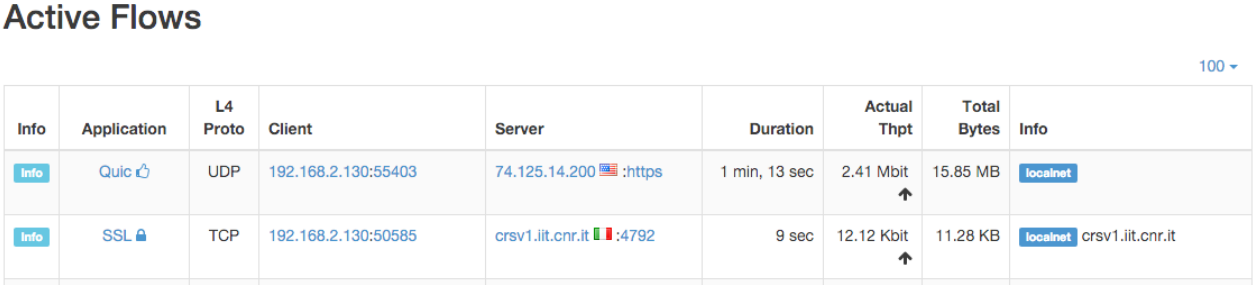
The Edit Traffic Profiles Page

In the screenshot above, ntopng has been configured with a profile that logically includes any kind of traffic having source and/or destination hosts within the private network 192.168.2.0/24.

Profiles must be expressed using the Berkeley Packet Filter (BPF) syntax. Filters will be parsed and syntax will be checked every time thew 'Save Profile' button is hit. Errors are raised when the syntax is not BPF compliant. A thorough discussion of the BPF falls outside the scope of this work. The interested reader is referred to http://biot.com/capstats/bpf.html for a detailed description of the syntax.

Realtime Profiles

Profiles are fine grained and potentially apply to every flow detected. Real time flows and their assigned profiles can be seen using the 'Flows' menu entry in the top toolbar. Similarly, profiles can be seen on a host basis by selecting the tab 'Flows' from the contextual Host Details menu.
A blue badge labelled with profile name will appear in the rightmost column 'Info' of every profiled flow.
In the example below are shown two currently active flows for host 192.168.2.130, that match the defined *localnet* profile.

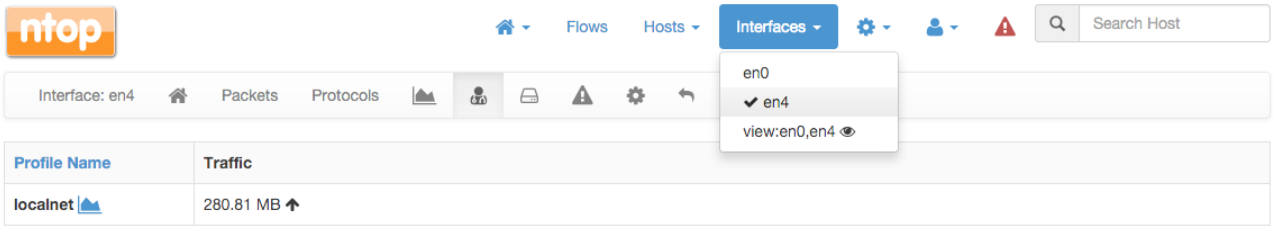


Traffic Profiles in the Active Flows Page

Historical Profiles Statistics

Profiles are not only available in realtime. Their traffic statistics are sampled every minute and stored in RRDs. Similarly, if ntopng was started with the *-F* modifier, flows will be exported to MySQL or ElasticSearch together with their profiles.

Historical charts and tables are available in the 'Profile Details' page, reachable from the 'Interface' contextual toolbar. By clicking on the doctor icon, it is possible to see the full list of profiles detected for the selected interface, together with their traffic and throughput trend. Profile Details page can be opened for each profile simply by clicking on the icon.



The Traffic Profiles Summary Page

Profile Details page shows historical profile traffic. An optional table with historical flow details — for flows matching the selected profile — is shown below the chart if ntopng was started with the *-F* modifier.

The Traffic Profile Details Page

Presently, no overlapping profiles are handled. This means that when a flow matches more than one traffic profile, it will be assigned to one profile only in a non-predictable way.

Bridging and Traffic Policing/Shaping

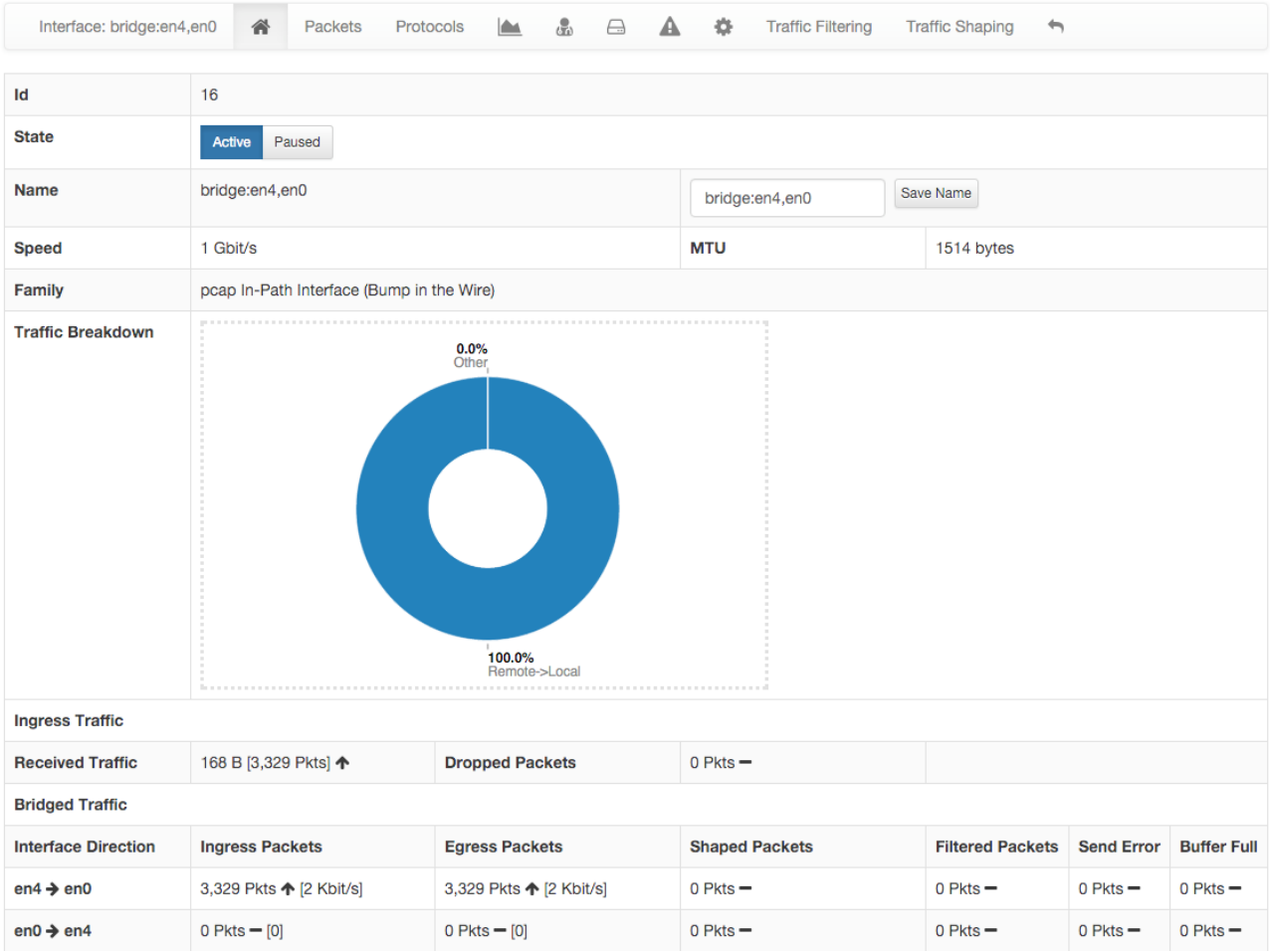
The Professional version of ntopng can operate as an active traffic monitor. Thus, ntopng is not only able to see *what* is flowing in the network, it is also able to shape and apply filtering policies to traffic flows.

To be able to operate as an active monitor, ntopng requires at least one bridge between a pair of physical interfaces. Bridges are specified via command line (or configuration file), using the same *-i* modified that is used for physical interfaces. An extra *bridge:* string must be added right after the -i modifier to tell ntopng that it is going to read a bridge. Physical interfaces must be indicated in a comma separated list that follows the *bridge:* string.

For example, the following line is to start ntopng and bridge together interfaces en0 and en4

```
ntopng -i bridge:en0,en4
```

Upon successful startup, ntopng shows bringing status and information in the bridged Interface Details page, reachable from the 'Interfaces' top toolbar menu.

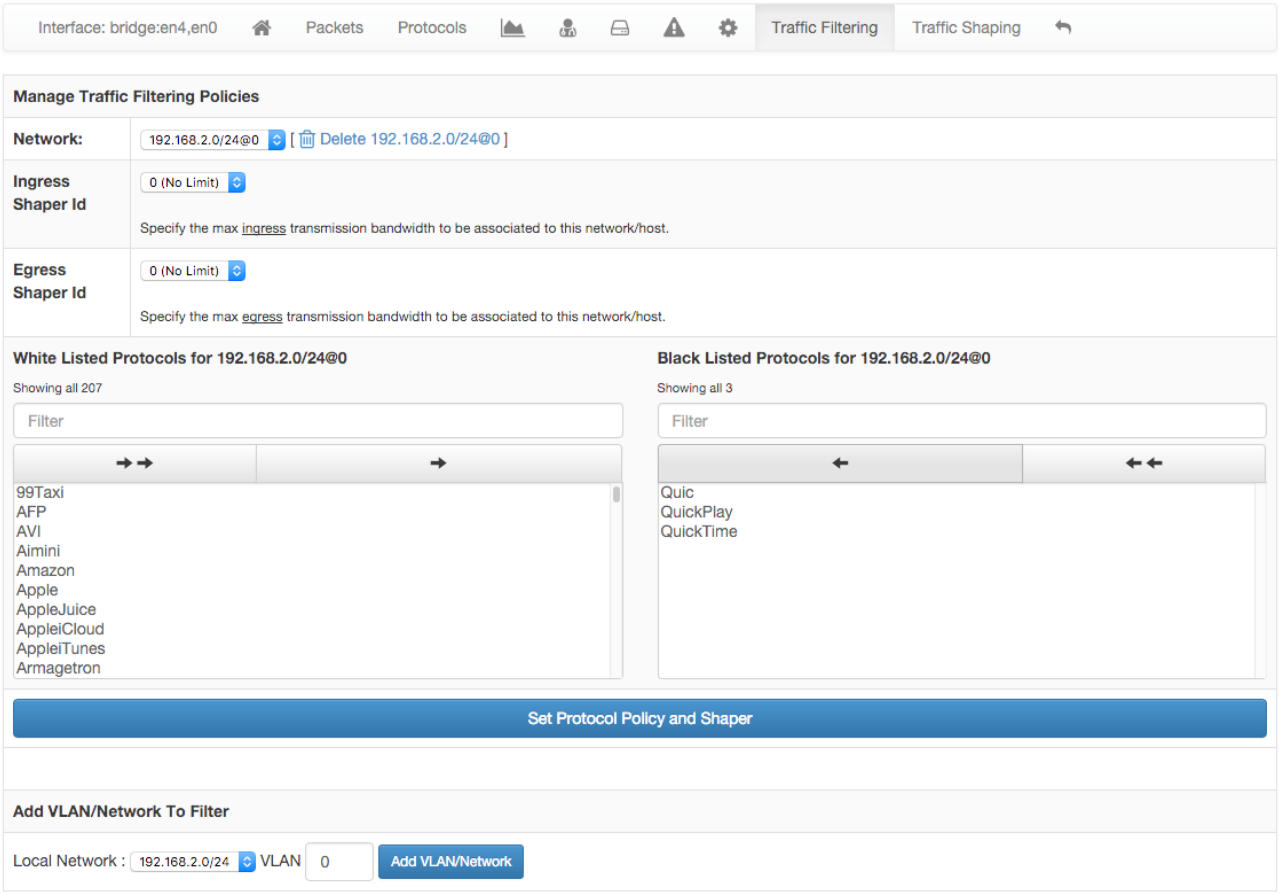


A Bridged Interface Details Page

Bridge information is given for each direction at the bottom of the page. Two additional entries appear in the contextual interface menu, namely Traffic Filtering and Traffic Shaping.

Traffic Filtering

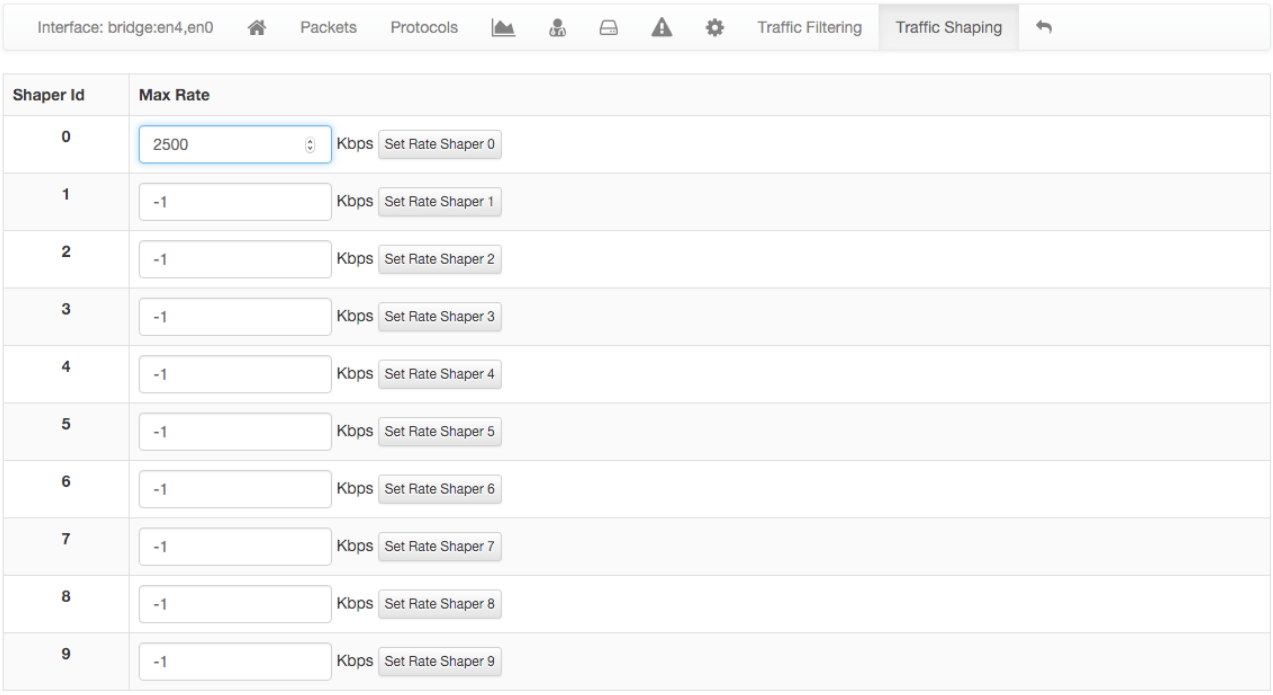
Traffic Filtering page allows to select shaping and filtering policies for each Local Network. Virtual LANs (VLANs) are supported as well. At the bottom of the page one can choose which local network / VLAN to apply filters and shapers to. Shapers regulate the maximum ingress and egress bandwidth allowed. Similarly, white- and black-lists enable the user to choose which applications are accepted and which must be dropped.



Traffic Filtering Page

Traffic Shaping

A pool of 10 different traffic shapers can be configured from the Traffic Shaping page. Each shaper accept a maximum rate, expressed in Kilobytes per second (Kbps). The 0 value is reserved to drop all traffic. The -1 disables shaping. Shapers configured here will be available — and identified by their Shaper Id — on page Traffic Filtering as Ingress and Egress shapers.



Shapers Configuration Page

Flows Dump

Ntopng can dump expired flow information either to a MySQL database or ElasticSearch. Ntopng is instructed to dump expired flows to MySQL via the -F startup modifier.

MySQL

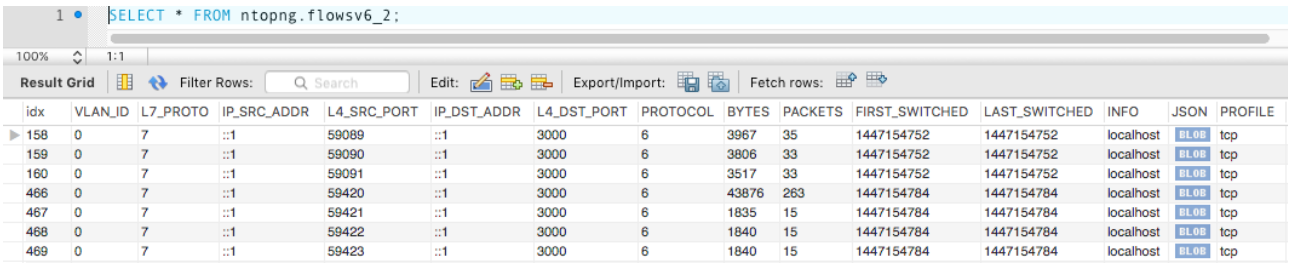
To dump expired flows to MySQL ntopng requires the -F modifier followed by a string in the following format

```
mysql;<host|socket>;<dbname>;<table name>;<user>;<pw>
```

The string has 6 semi-colon separated fields

- `mysql` tells ntopng to dump flows to MySQL
- `<host|socket>` is the host (or the socket) of a running MySQL instance that will receive expired flows
- `<dbname>` specify the name of the MySQL database to use. If the database does not exist, ntopng will create it.
- `<table name>` specify the prefix of MySQL table names to use. Presently the prefix is always defaulted to `flows`.
- `<user>;<pw>` are the credential of a MySQL user that has privileges to create, select and update tables on `<dbname>`.

Ntopng creates two database tables. Tables are named `flowsv4` and `flowsv6` that are used to store IPv4 and IPv6 flows, respectively.



```
1 • SELECT * FROM ntopng.flowsv6_2;
```

100% 1:1

Result Grid | Filter Rows: Search | Edit: | Export/Import: | Fetch rows:

idx	VLAN_ID	L7_PROTO	IP_SRC_ADDR	L4_SRC_PORT	IP_DST_ADDR	L4_DST_PORT	PROTOCOL	BYTES	PACKETS	FIRST_SWITCHED	LAST_SWITCHED	INFO	JSON	PROFILE
158	0	7	::1	59089	::1	3000	6	3967	35	1447154752	1447154752	localhost	BLOB	tcp
159	0	7	::1	59090	::1	3000	6	3806	33	1447154752	1447154752	localhost	BLOB	tcp
160	0	7	::1	59091	::1	3000	6	3517	33	1447154752	1447154752	localhost	BLOB	tcp
466	0	7	::1	59420	::1	3000	6	43876	263	1447154784	1447154784	localhost	BLOB	tcp
467	0	7	::1	59421	::1	3000	6	1835	15	1447154784	1447154784	localhost	BLOB	tcp
468	0	7	::1	59422	::1	3000	6	1840	15	1447154784	1447154784	localhost	BLOB	tcp
469	0	7	::1	59423	::1	3000	6	1840	15	1447154784	1447154784	localhost	BLOB	tcp

A MySQL Table with Dumped Flows

ElasticSearch

Elasticsearch is an Open-Source real-time search and analytics engine with a powerful RESTful API built on top of Apache Lucene. Ntopng can connect to an external Elasticsearch cluster as client using the Bulk insert API for JSON mapped indexing.

Elasticsearch is designed for quickly and dynamically analyzing or searching through large amounts of data and thus is ideal for flows generated by ntopng, enabling users and integrators to create a virtually infinite number and variety of statistics using Kibana.

To learn more about Elasticsearch visit: https://www.elastic.co/guide.

To dump expired flows to Elasticsearch ntopng requires the -F modifier followed by a string in the following format:

```
es;<idx type>;<idx name>;<es URL>;<http auth>
```

The string has 5 semi-colon separated fields

- `es` instructs ntopng to dump flows to Elasticsearch
- `<idx type>` "_type" to use in exported documents
- `<idx name>` index to use for exported documents [accepts strftime() format]
- `<es URL>` URL of Elasticsearch Bulk API [ie: http://127.0.0.1:9200/bulk]
- `<http auth>` Basic HTTP Authentication [username:password]

Example:

```
es;ntopng;ntopng-%Y.%m.%d;http://localhost:9200/_bulk;
```

Definitions:

Indexes are like 'databases' in a RDBMS terms. An index is a logical namespace which maps to one or more primary shards and can have zero or more replica shards distributed across nodes of a cluster. Index mapping defines the multiple supported types.

Mapping is required for Elasticsearch to correctly interpret all fields produced by ntopng, specifically those containing IP and Geo Location data. This is achieved by using a mapping template for ntop types, automatically inserted by the application at startup. Note this action requires full admin rights on the cluster in order to be performed successfully.

Ntopng will create Indexes and Mapping automatically on startup with no action required.
Each time the index name changes, a new Index is created. By default, ntopng creates one daily index (i.e.: ntopng-2015.11.21). Index types can be used to differentiate instances.

Data Rotation:

The official Curator tool from Elastic can be used to manage and rotate Indexes created by ntopng according to the user preferences and requirements.

Additional ntopng Features

Ntopng has several additional features that fall outside the scope of this user guide. New features are always under active development and include

- Ability to work in inline mode and enforce traffic and layer-7 protocols
- Embedded-Systems aware including Raspberry Pi and Ubiquity Networks

Please stay tuned and follow the ntop blog (http://blog.ntop.org) for all the latest news or visit the ntop Github page at http://github.com/ntop.