Monitoraggio di Rete con ntopng

Luca Deri <deri@ntop.org>

Outlook

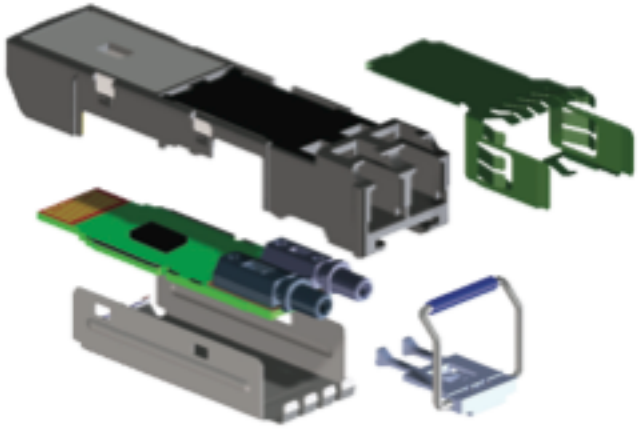
- What are the main activities of ntop.org ?
- ntop's view on network monitoring.
- From ntop to ntopng.
- ntopng architecture and design.
- Using ntopng.
- Advanced monitoring with ntopng.
- Future roadmap items.

About ntop.org [1/2]

- Private company devoted to development of open source network traffic monitoring applications.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.
- Today our products range from traffic monitoring, high-speed packet processing, deep-packet inspection, and IDS/IPS acceleration.

About ntop.org [2/2]

- Our software is powering many commercial products...



Integrated ASIC with JDSU technology

ntop Goals

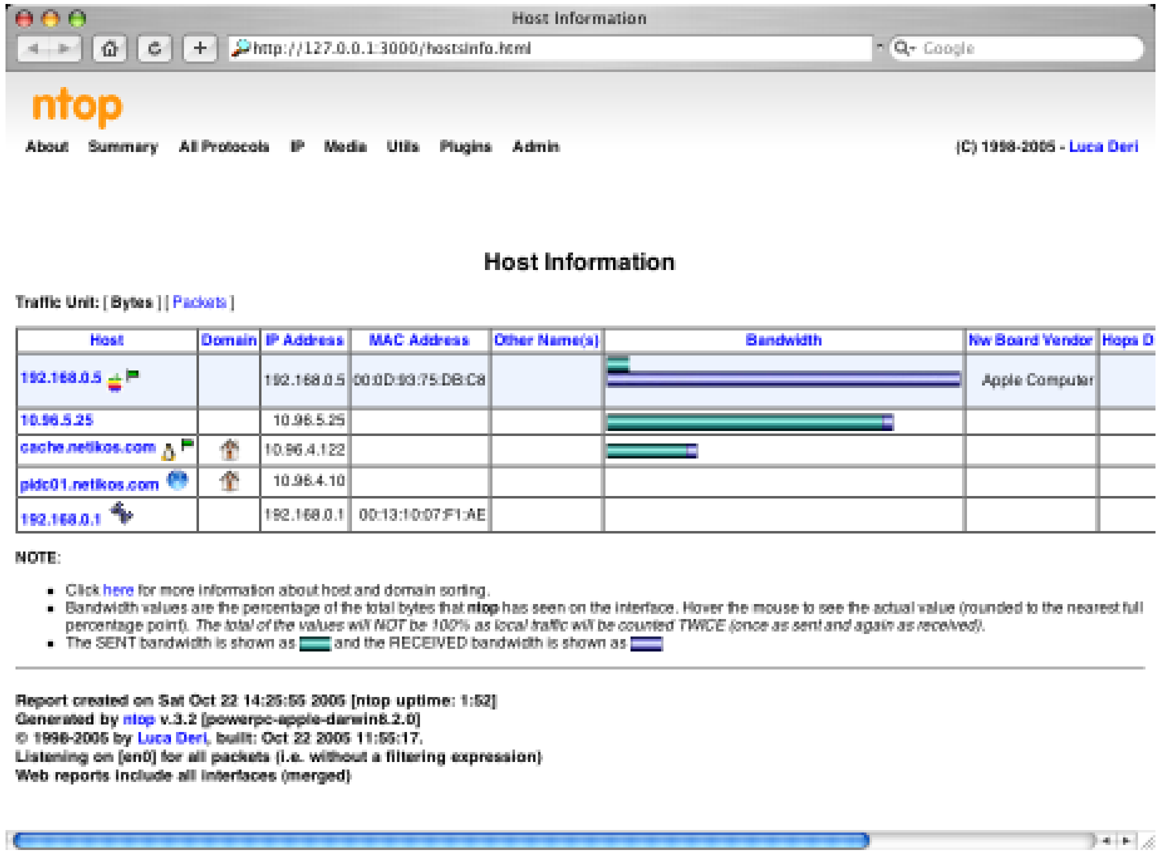
- Provide better, yet price effective, traffic monitoring solution by enabling users to have increased traffic visibility.
- Go beyond standard metrics and increase traffic visibility by analysing key protocols in detail.
- Provide users comprehensive and accurate traffic reports able to offer at a fraction of price what many commercial products do together.
- Promote open-source software, while protecting selected IPRs.

ntop's Approach to Traffic Monitoring

- Ability to capture, process and (optionally) transmit traffic at line rate, any packet size.
- Leverage on modern multi-core/NUMA architectures in order to promote scalability.
- Use commodity hardware for producing affordable, long-living (no vendor lock), scalable (use new hardware by the time it is becoming available) monitoring solutions.
- Use open-source to spread the software, and let the community test it on unchartered places.

Some History

- In 1998, the original ntop has been created.
- It was a C-based app embedding a web server able to capture traffic and analyse it.



Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Nw Board Vendor	Hops D
192.168.0.5		192.168.0.5	00:0D:93:75:DB:C8			Apple Computer	
10.96.5.25		10.96.5.25					
cache.netikos.com		10.96.4.122					
pidc01.netikos.com		10.96.4.10					
192.168.0.1		192.168.0.1	00:13:10:07:F1:AE				

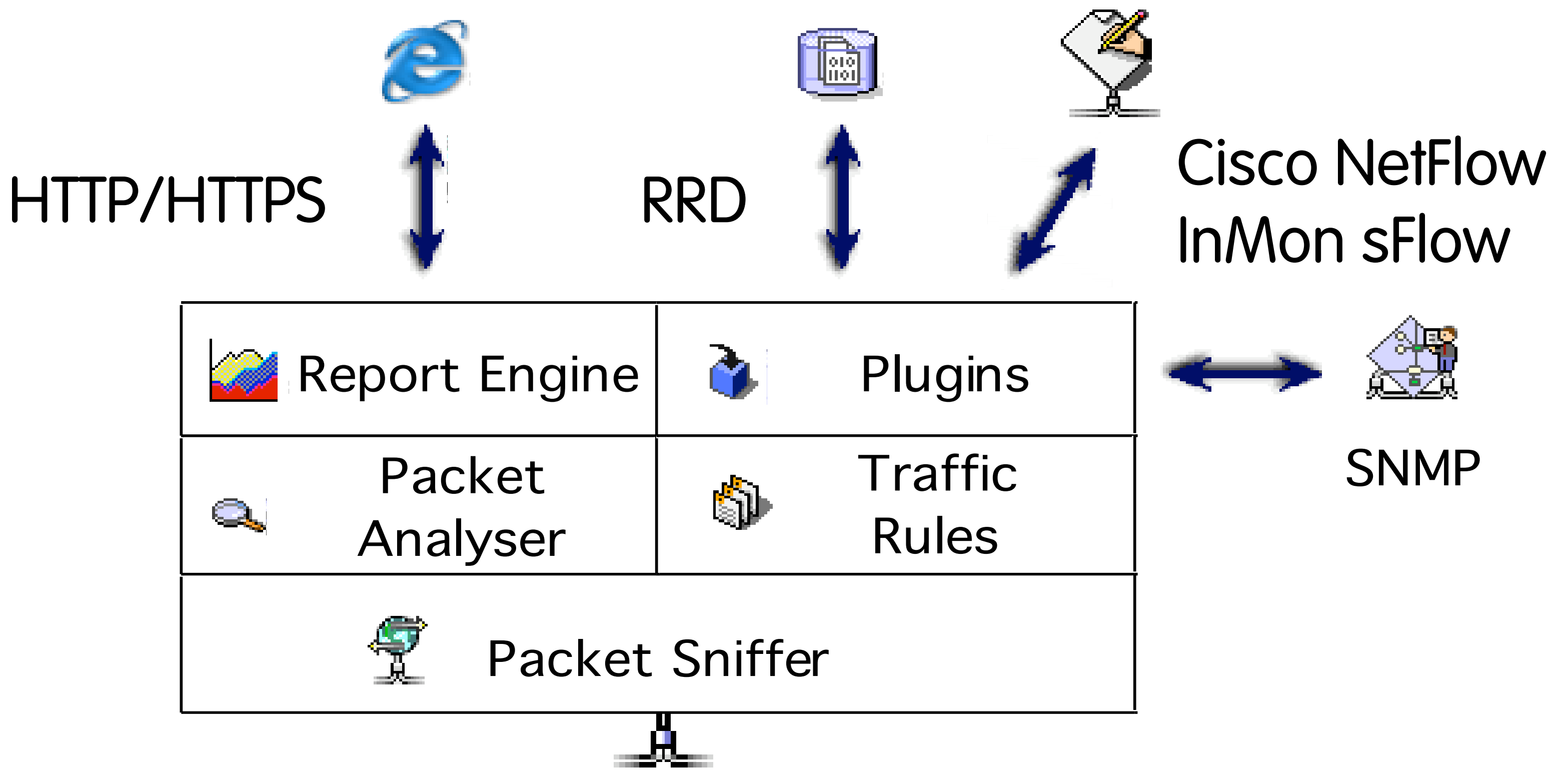
NOTE:

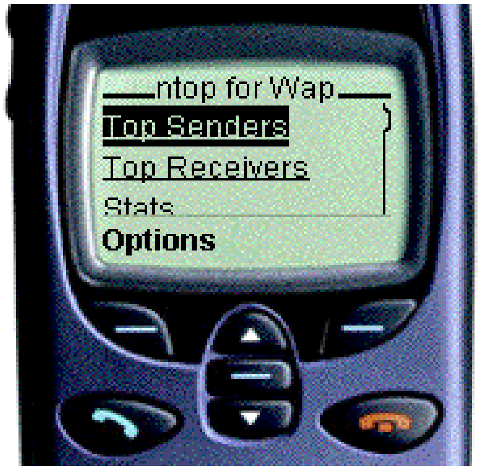
- Click here for more information about host and domain sorting.
- Bandwidth values are the percentage of the total bytes that **ntop** has seen on the interface. Hover the mouse to see the actual value (rounded to the nearest full percentage point). *The total of the values will NOT be 100% as local traffic will be counted TWICE (once as sent and again as received).*
- The SENT bandwidth is shown as 🟩 and the RECEIVED bandwidth is shown as 🟦

Report created on Sat Oct 22 14:25:55 2005 [ntop uptime: 1:52]
Generated by ntop v.3.2 [powerpc-apple-darwin8.2.0]
© 1998-2005 by Luca Deri, built: Oct 22 2005 11:55:17.
Listening on [en0] for all packets (i.e. without a filtering expression)
Web reports include all interfaces (merged)

- Contrary to many tools available at that time, ntop used a web GUI to report traffic activities.
- It is available for Unix and Windows under GPL.

ntop Architecture



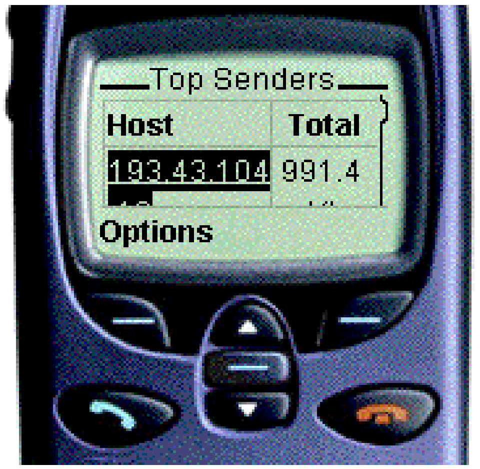

ntop for Wap

Top Senders

Top Receivers

Stats

Options


Top Senders

Host	Total
193.43.104	991.4

Options

Host 131.114.20.3

Name	ibook
Sent	312.5Kb

Why was ntop obsolete?

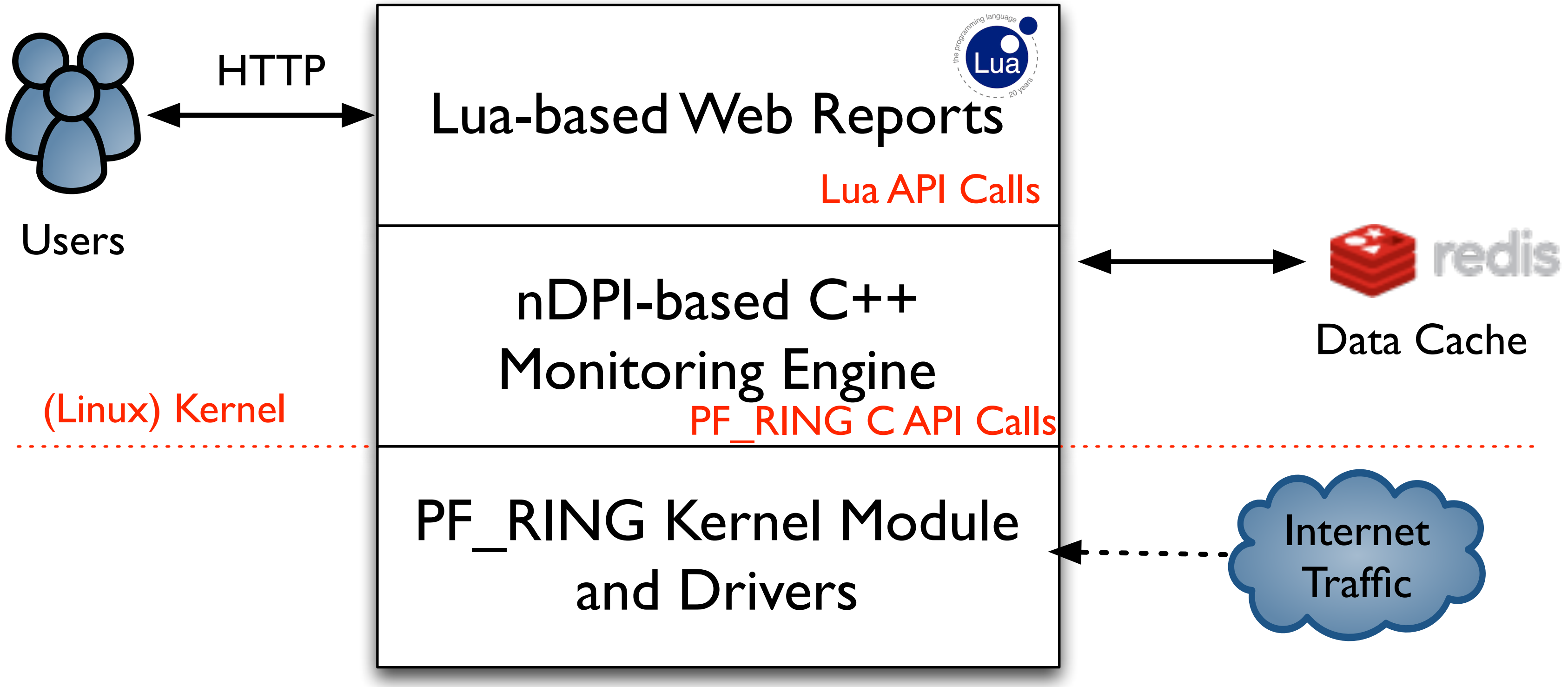
- Its original LAN-oriented design prevented ntop from handling more than a few hundred Mbit.
- The GUI was an old (no fancy HTML 5) monolithic piece written in C so changing/extending a page required a programmer.
- ntop could not be used as web-less monitoring engine to be integrated with other apps.
- Many components were designed in 1998, and it was time to start over (spaghetti code).

ntopng Design Goals

- Clean separation between the monitoring engine and the reporting facilities.
- Robust, crash-free engine (ntop was not really so).
- Platform scriptability for enabling extensions or changes at runtime without restart.
- Realtime: most monitoring tools aggregate data (5 mins usually) and present it when it's too late.
- Many new features including HTML 5-based dynamic GUI, categorization, DPI.

ntopng Architecture

- Three different and self-contained components, communicating with clean API calls.



ntopng Monitoring Engine

- Coded in C++ and based the concept of flow (set of packets with the same 6-tuple).
- Flows are inspected with a home-grown DPI-library named nDPI aiming to discover the “real” application protocol (no ports are used).
- Information is clustered per:
  - (Capture) Network Device
  - Flow
  - Host
  - High-level Aggregations

Information Lifecycle

- All information (e.g. hosts and flows) is stored in memory.
- Using command line options, users can specify how many hosts/flows can be kept in memory.
- Idle flows are periodically purged in order to free memory.
- Hosts are serialised and stored in JSON format in Redis for 1 hour, so that in case new traffic is detected ntopng can restore them from cache.

Packet Processing Journey

1. Packet capture: PF_RING (Linux) or libpcap.
2. Packet decoding: no IP traffic is accounted.
3. IPv4/v6 Traffic only:
   1. Map the packet to a 6-tuple flow and increment stats.
   2. Identify source/destination hosts and increment stats.
   3. Use nDPI to identify the flow application protocol
      1. UDP flows are identified in no more than 2 packets.
      2. TCP Flows can be identified in up to 15 packets in total, otherwise the flow is marked as “Unknown”.
4. Move to the next packet.

The need for DPI in Monitoring [1/2]

- Limit traffic analysis at packet header level it is no longer enough (nor cool).
- Network administrators want to know the real protocol without relying on the port being used.
- Selected protocols can be “precisely dissected” (e.g. HTTP) in order to extract information, but on the rest of the traffic it is necessary to tell network administrators what is the protocol flowing in their network.

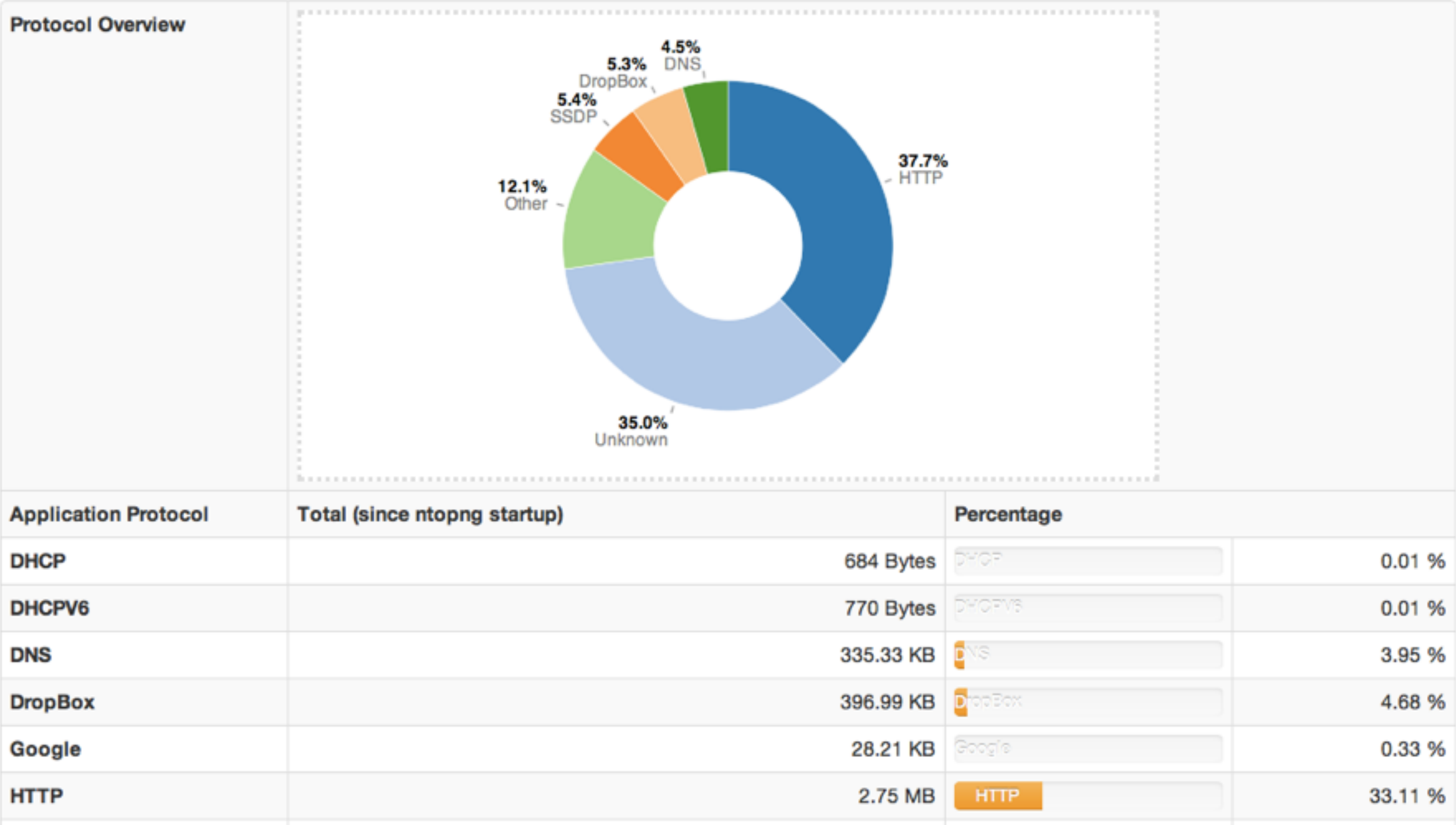
The need for DPI in Monitoring [2/2]

- DPI (Deep Packet Inspection) is a technique for inspecting the packet payload for the purpose of extracting metadata (e.g. protocol).
- There are many DPI toolkits available but they are not what we looked for as:
  - They are proprietary (you need to sign an NDA to use them), and costly for both purchase and maintenance.
  - Adding a new protocol requires vendor support (i.e. it has a high cost and might need time until the vendor supports it) = you're locked-in.
- On a nutshell DPI is a requirement but the market does not offer an alternative for open-source.

Say hello to nDPI

- ntop has decided to develop its own GPL DPI toolkit in order to build an open DPI layer for ntop and third party applications.
- Supported protocols (~170) include:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
  - Business (VNC, RDP, Citrix, *SQL)

nDPI on ntopng: Sample Report



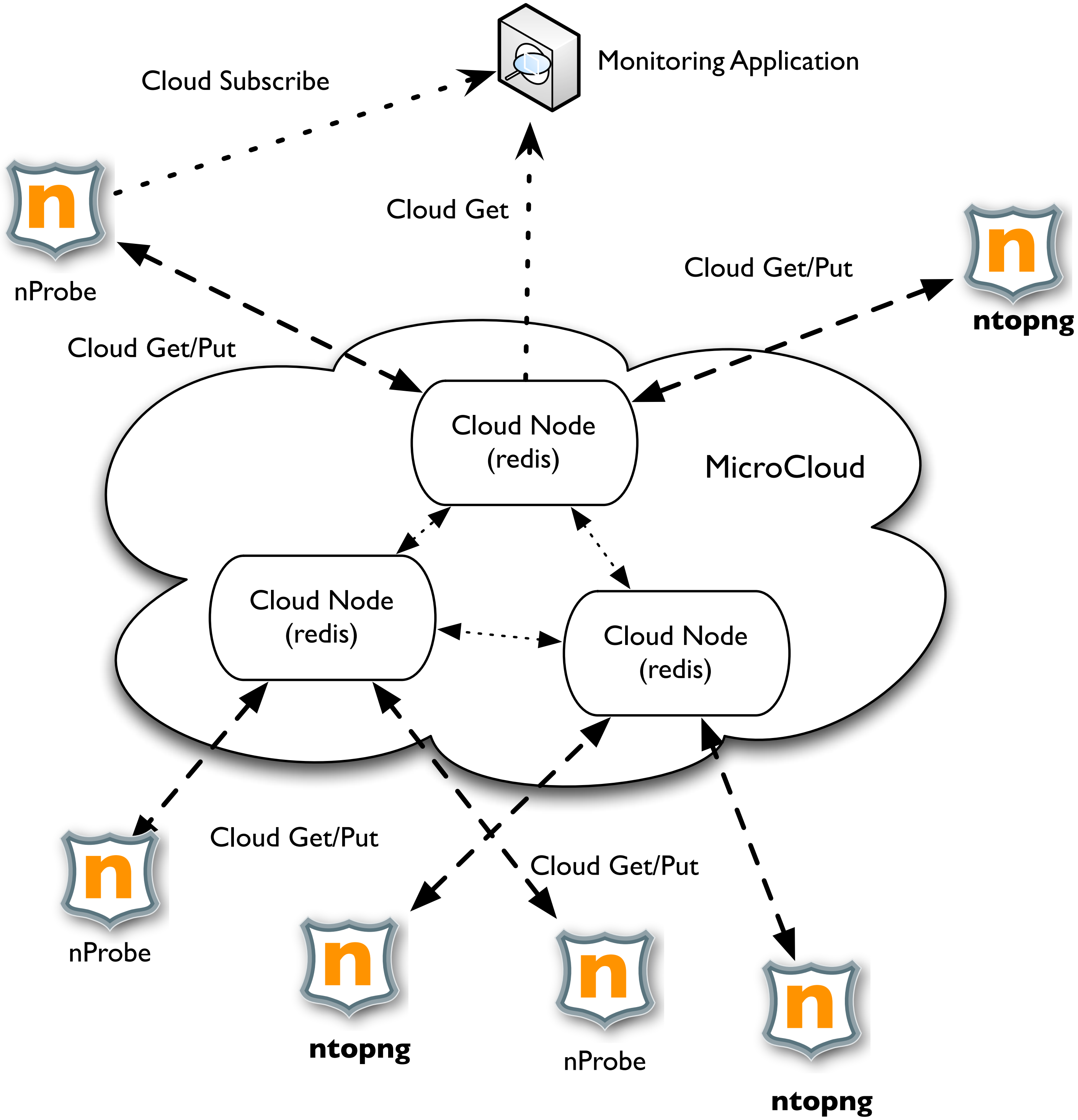
Protocol Overview

Application Protocol	Total (since ntopng startup)	Percentage	
DHCP	684 Bytes	DHCP	0.01 %
DHCPV6	770 Bytes	DHCPV6	0.01 %
DNS	335.33 KB	DNS	3.95 %
DropBox	396.99 KB	DropBox	4.68 %
Google	28.21 KB	Google	0.33 %
HTTP	2.75 MB	HTTP	33.11 %

ntopng and Redis

- Redis is an open source key-value in-memory database.
- ntop uses it to cache data such as:
    - Configuration and user preferences information.
    - DNS name resolution (numeric to symbolic).
    - Volatile monitoring data (e.g. hosts JSON representation).
- Some information is persistent (e.g. preferences) and some is volatile: ntopng can tell redis how long a given value must be kept in cache.

Welcome to the MicroCloud

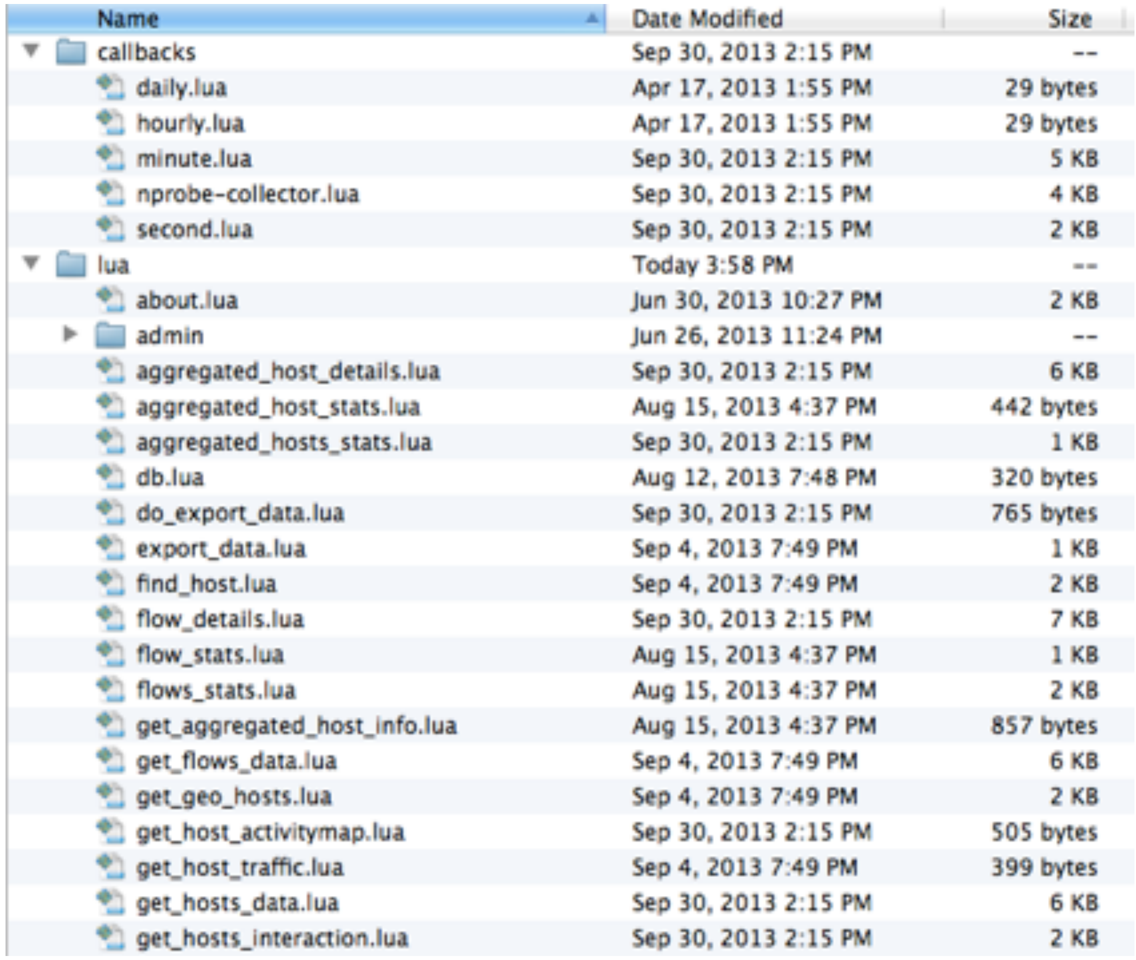


Lua-based ntopng Scriptability [1/3]

- A design principle of ntopng has been the clean separation of the GUI from engine (in ntop it was all mixed).
- This means that ntopng can (also) be used (via HTTP) to feed data into third party apps such as Nagios or OpenNMS.
- All data export from the engine happens via Lua.
- Lua methods invoke the ntopng C++ API in order to interact with the monitoring engine.

Lua-based ntopng Scriptability [2/3]

- `/scripts/callback/` scripts are executed periodically to perform specific actions.
- `/scripts/lua/` scripts are executed only by the web GUI.
- Example:
  `http://ntopng:3000/lua/flow_stats.lua`



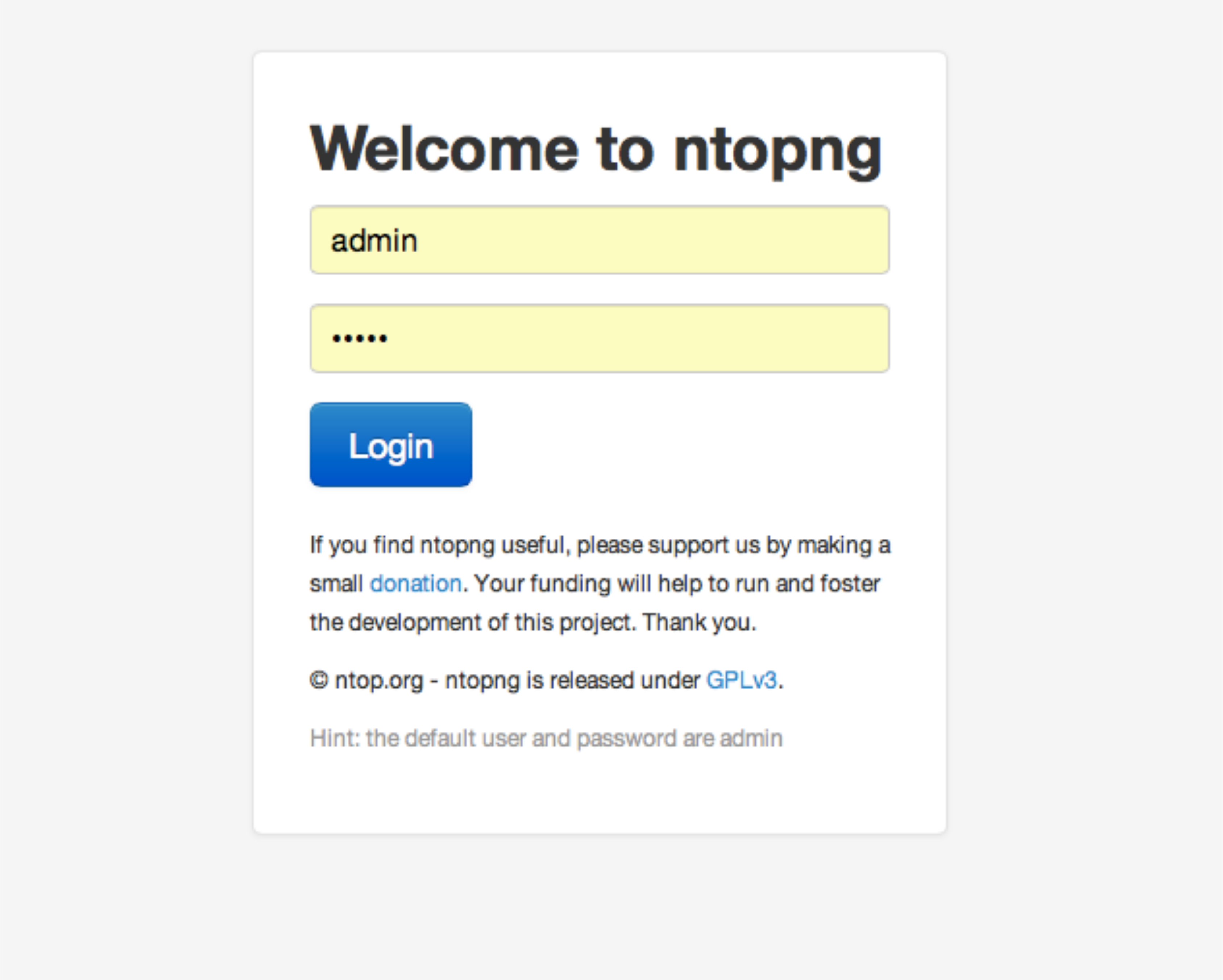
Name	Date Modified	Size
▼ callbacks	Sep 30, 2013 2:15 PM	--
daily.lua	Apr 17, 2013 1:55 PM	29 bytes
hourly.lua	Apr 17, 2013 1:55 PM	29 bytes
minute.lua	Sep 30, 2013 2:15 PM	5 KB
nprobe-collector.lua	Sep 30, 2013 2:15 PM	4 KB
second.lua	Sep 30, 2013 2:15 PM	2 KB
▼ lua	Today 3:58 PM	--
about.lua	Jun 30, 2013 10:27 PM	2 KB
▶ admin	Jun 26, 2013 11:24 PM	--
aggregated_host_details.lua	Sep 30, 2013 2:15 PM	6 KB
aggregated_host_stats.lua	Aug 15, 2013 4:37 PM	442 bytes
aggregated_hosts_stats.lua	Sep 30, 2013 2:15 PM	1 KB
db.lua	Aug 12, 2013 7:48 PM	320 bytes
do_export_data.lua	Sep 30, 2013 2:15 PM	765 bytes
export_data.lua	Sep 4, 2013 7:49 PM	1 KB
find_host.lua	Sep 4, 2013 7:49 PM	2 KB
flow_details.lua	Sep 30, 2013 2:15 PM	7 KB
flow_stats.lua	Aug 15, 2013 4:37 PM	1 KB
flows_stats.lua	Aug 15, 2013 4:37 PM	2 KB
get_aggregated_host_info.lua	Aug 15, 2013 4:37 PM	857 bytes
get_flows_data.lua	Sep 4, 2013 7:49 PM	6 KB
get_geo_hosts.lua	Sep 4, 2013 7:49 PM	2 KB
get_host_activitymap.lua	Sep 30, 2013 2:15 PM	505 bytes
get_host_traffic.lua	Sep 4, 2013 7:49 PM	399 bytes
get_hosts_data.lua	Sep 30, 2013 2:15 PM	6 KB
get_hosts_interaction.lua	Sep 30, 2013 2:15 PM	2 KB

Lua-based ntopng Scriptability [3/3]

- ntopng defines (in C++) two Lua classes:
  - `interface`
    - Hook to objects that describe flows and hosts.
    - Access to live monitoring data.
  - `ntop`
    - General functions used to interact with ntopng configuration.
- Lua objects are usually in “read-only” mode
  - C++ sets their data, Lua reads data (e.g. `host.name`).
  - Some Lua methods (e.g. `interface.restoreHost()`) can however modify the information stored in the engine.

Using ntopng

Logging into ntopng



Welcome to ntopng

admin

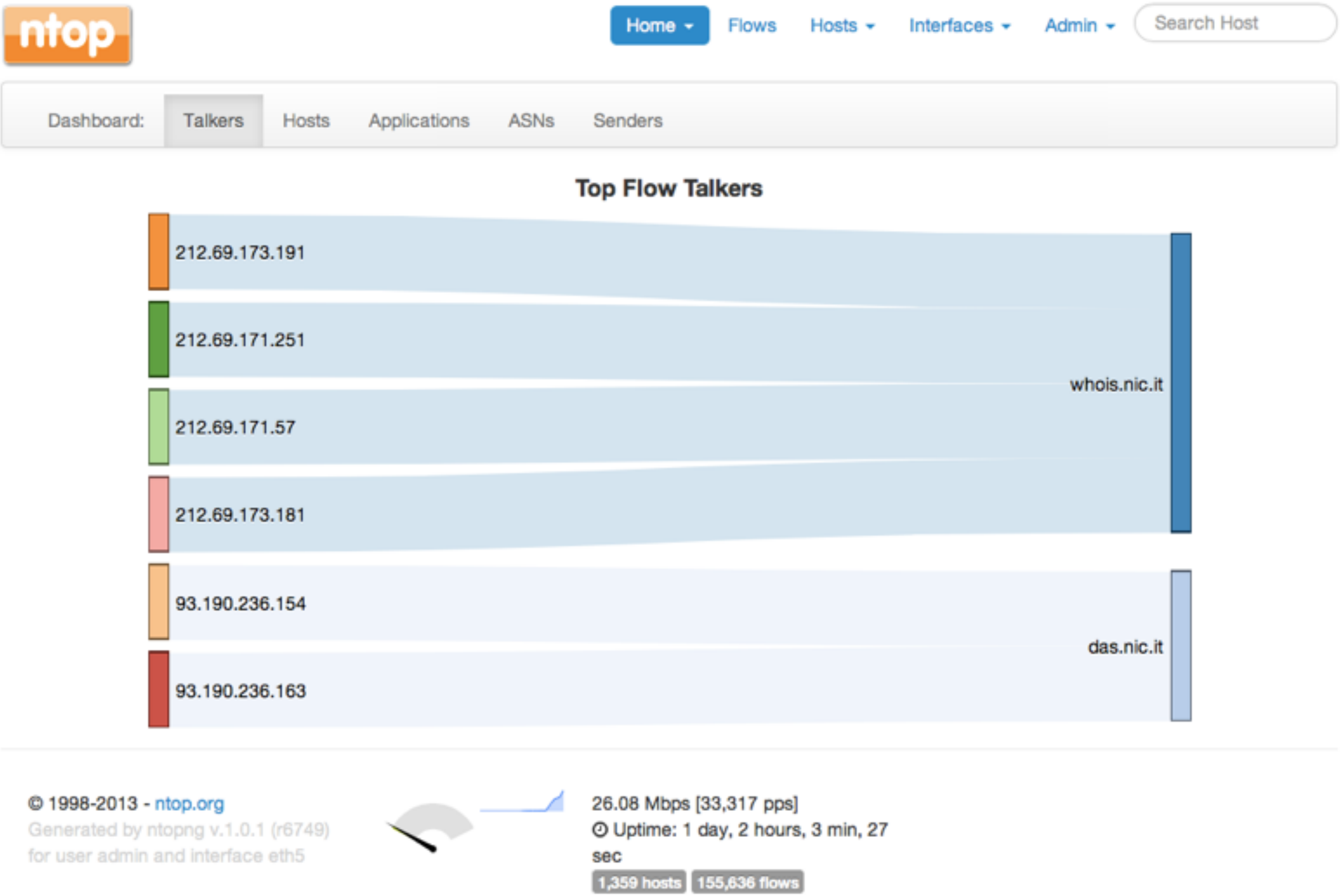
•••••

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.

© ntop.org - ntopng is released under GPLv3.

Hint: the default user and password are admin

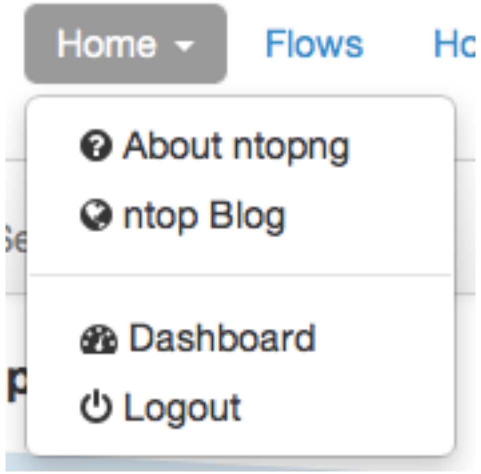
Dashboard

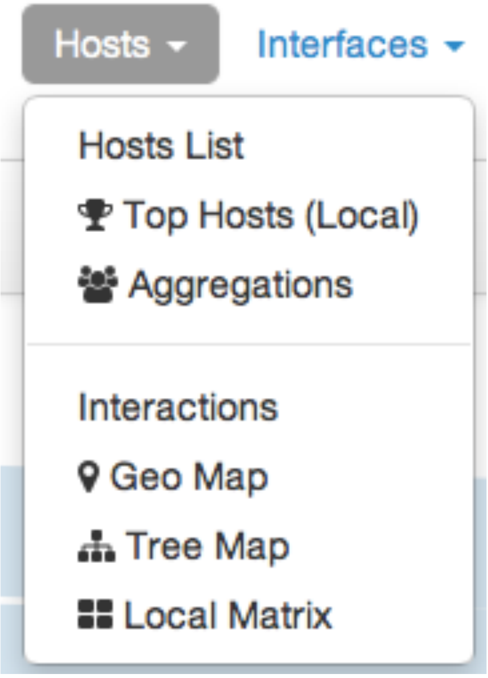


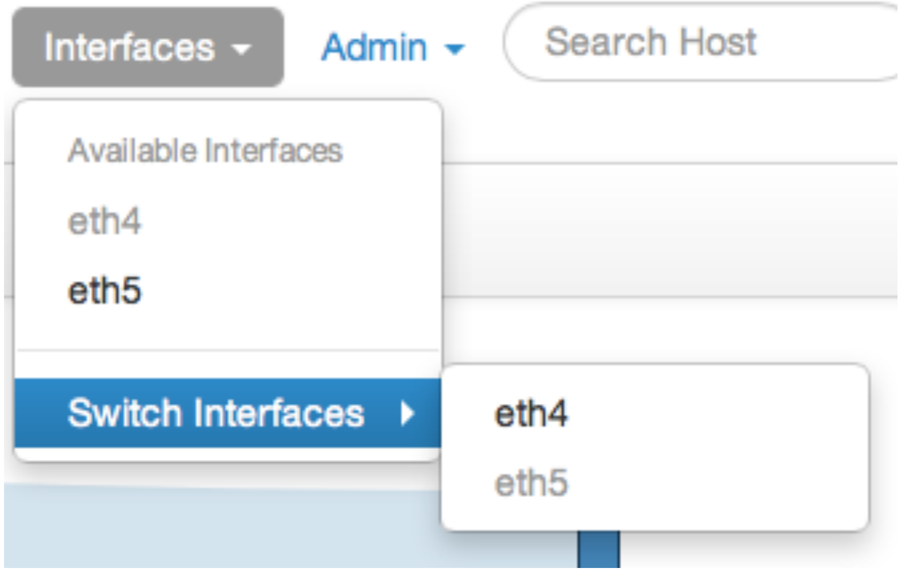
© 1998-2013 - ntop.org
Generated by ntopng v.1.0.1 (r6749)
for user admin and interface eth5

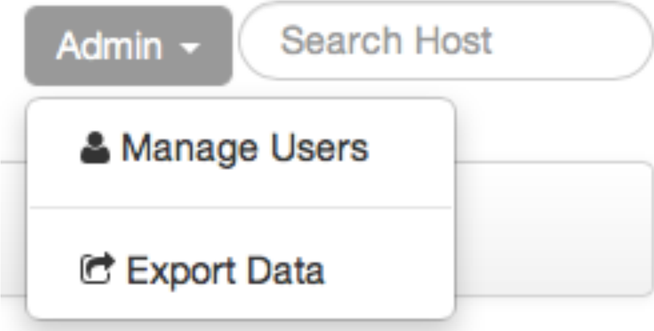
26.08 Mbps [33,317 pps]
Uptime: 1 day, 2 hours, 3 min, 27 sec
1,359 hosts 155,636 flows

Available Menu Items

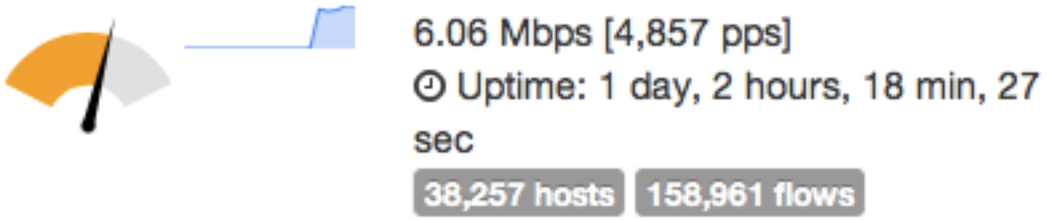








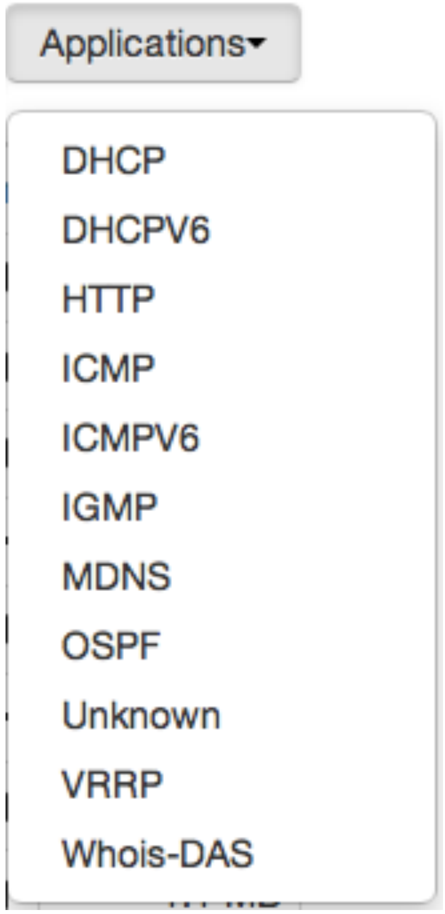
Dynamic Web Interface

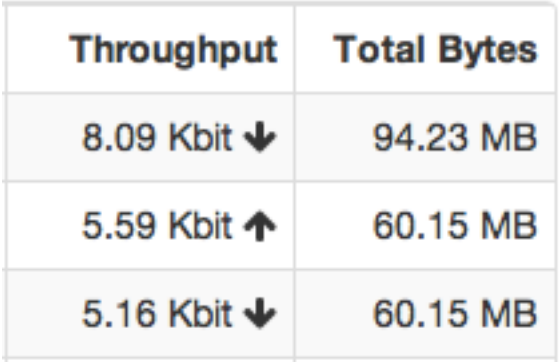


6.06 Mbps [4,857 pps]

Uptime: 1 day, 2 hours, 18 min, 27 sec

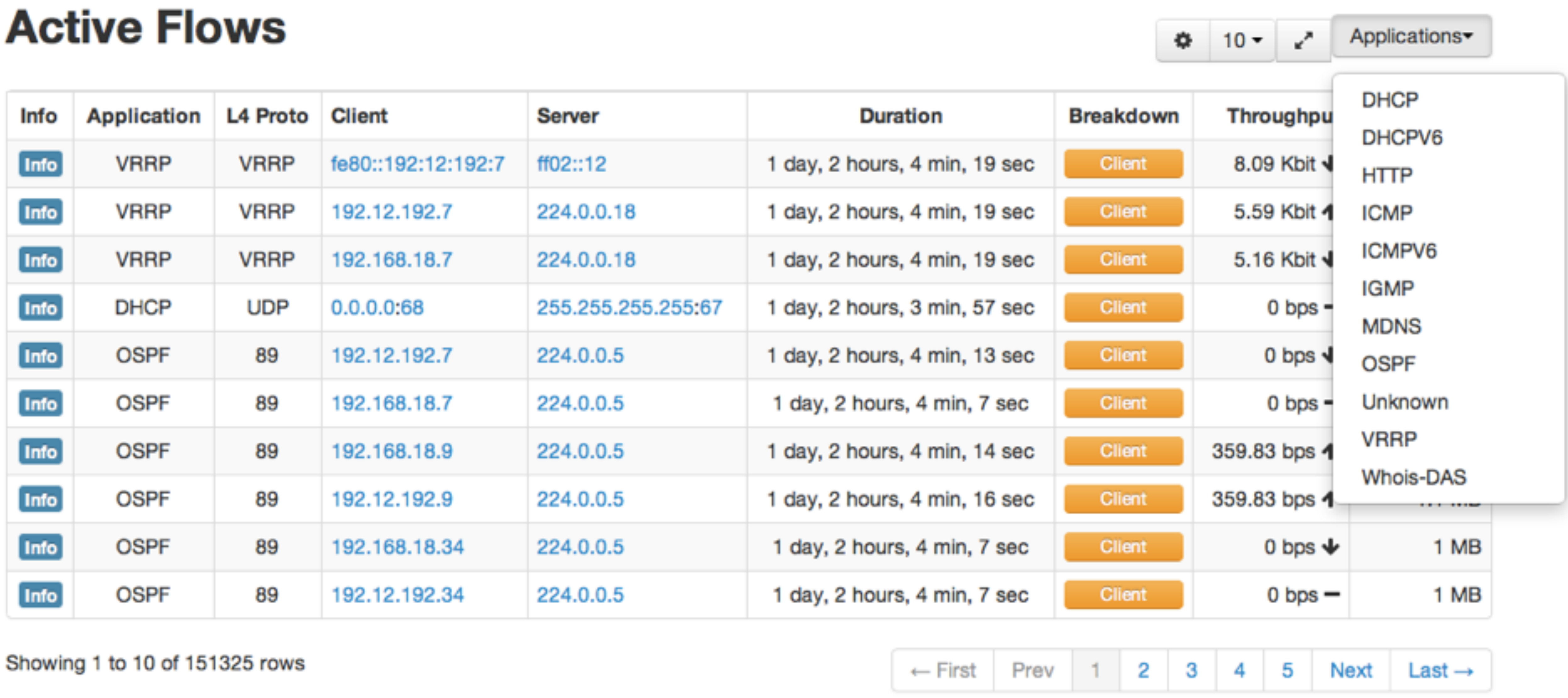
38,257 hosts 158,961 flows





Throughput	Total Bytes
8.09 Kbit ↓	94.23 MB
5.59 Kbit ↑	60.15 MB
5.16 Kbit ↓	60.15 MB

Flows Monitoring [1/2]

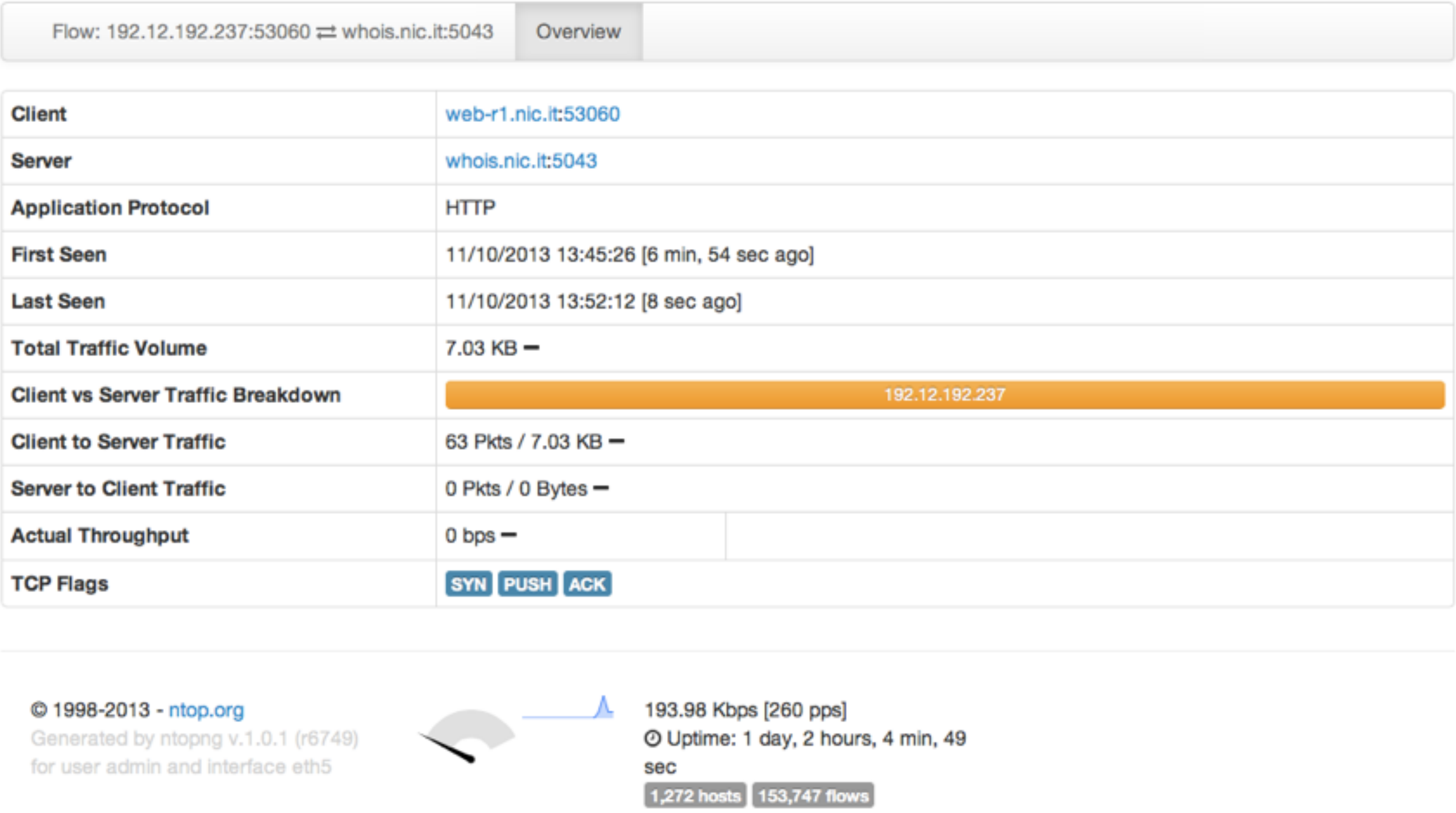


Active Flows

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Throughpu	
Info	VRRP	VRRP	fe80::192:12:192:7	ff02::12	1 day, 2 hours, 4 min, 19 sec	Client	8.09 Kbit ↓	
Info	VRRP	VRRP	192.12.192.7	224.0.0.18	1 day, 2 hours, 4 min, 19 sec	Client	5.59 Kbit ↑	
Info	VRRP	VRRP	192.168.18.7	224.0.0.18	1 day, 2 hours, 4 min, 19 sec	Client	5.16 Kbit ↓	
Info	DHCP	UDP	0.0.0.0:68	255.255.255.255:67	1 day, 2 hours, 3 min, 57 sec	Client	0 bps –	
Info	OSPF	89	192.12.192.7	224.0.0.5	1 day, 2 hours, 4 min, 13 sec	Client	0 bps ↓	
Info	OSPF	89	192.168.18.7	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps –	
Info	OSPF	89	192.168.18.9	224.0.0.5	1 day, 2 hours, 4 min, 14 sec	Client	359.83 bps ↑	
Info	OSPF	89	192.12.192.9	224.0.0.5	1 day, 2 hours, 4 min, 16 sec	Client	359.83 bps ↑	[illegible] MB
Info	OSPF	89	192.168.18.34	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps ↓	1 MB
Info	OSPF	89	192.12.192.34	224.0.0.5	1 day, 2 hours, 4 min, 7 sec	Client	0 bps –	1 MB

Showing 1 to 10 of 151325 rows

Flows Monitoring [2/2]



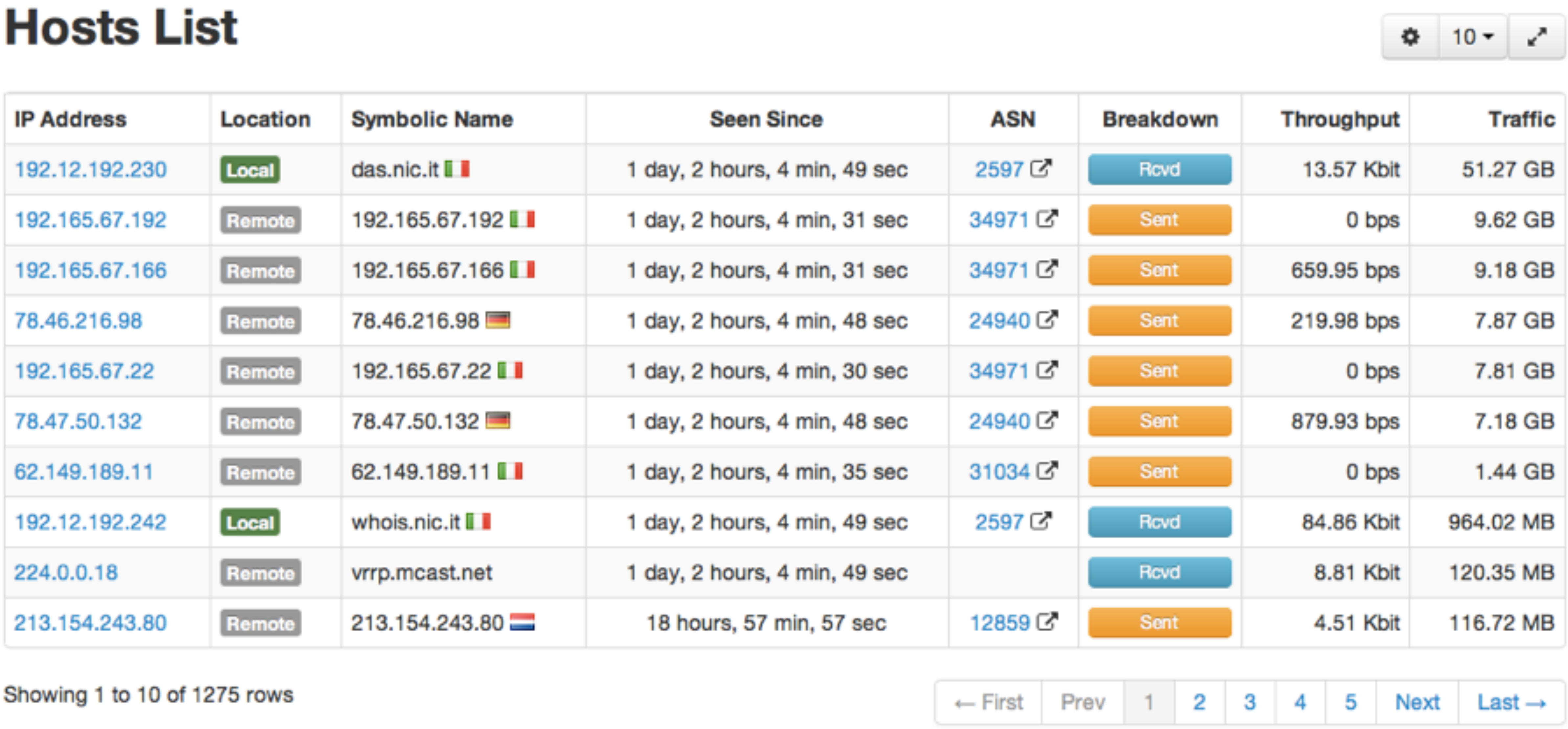
Flow: 192.12.192.237:53060 ⇄ whois.nic.it:5043 | Overview

Client	web-r1.nic.it:53060
Server	whois.nic.it:5043
Application Protocol	HTTP
First Seen	11/10/2013 13:45:26 [6 min, 54 sec ago]
Last Seen	11/10/2013 13:52:12 [8 sec ago]
Total Traffic Volume	7.03 KB —
Client vs Server Traffic Breakdown	192.12.192.237
Client to Server Traffic	63 Pkts / 7.03 KB —
Server to Client Traffic	0 Pkts / 0 Bytes —
Actual Throughput	0 bps —
TCP Flags	SYN PUSH ACK

© 1998-2013 - ntop.org
Generated by ntopng v.1.0.1 (r6749)
for user admin and interface eth5

193.98 Kbps [260 pps]
Uptime: 1 day, 2 hours, 4 min, 49 sec
1,272 hosts 153,747 flows

Host Monitoring [1/3]

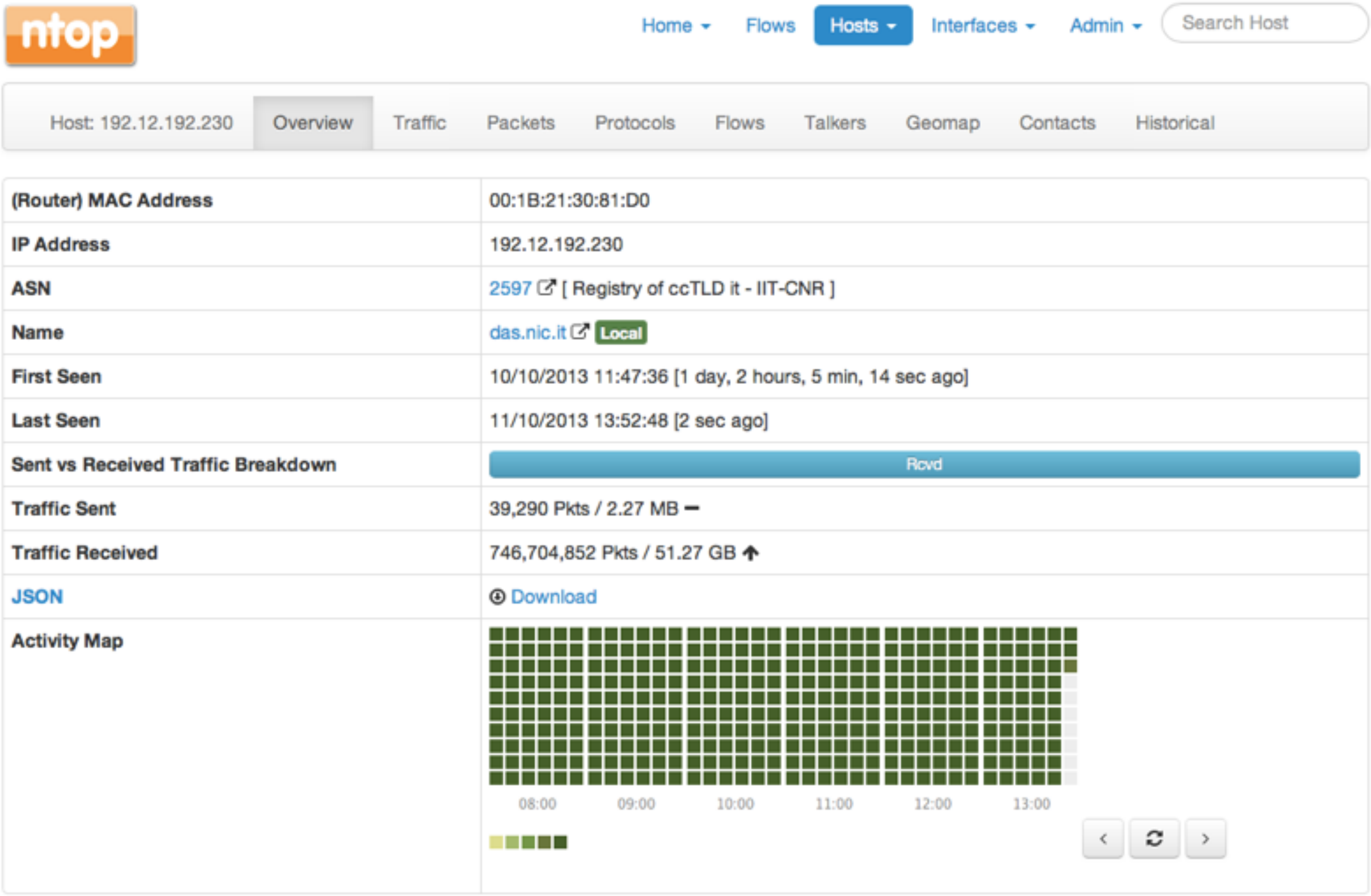


Hosts List

IP Address	Location	Symbolic Name	Seen Since	ASN	Breakdown	Throughput	Traffic
192.12.192.230	Local	das.nic.it 🇮🇹	1 day, 2 hours, 4 min, 49 sec	2597 ↗	Rcvd	13.57 Kbit	51.27 GB
192.165.67.192	Remote	192.165.67.192 🇮🇹	1 day, 2 hours, 4 min, 31 sec	34971 ↗	Sent	0 bps	9.62 GB
192.165.67.166	Remote	192.165.67.166 🇮🇹	1 day, 2 hours, 4 min, 31 sec	34971 ↗	Sent	659.95 bps	9.18 GB
78.46.216.98	Remote	78.46.216.98 🇩🇪	1 day, 2 hours, 4 min, 48 sec	24940 ↗	Sent	219.98 bps	7.87 GB
192.165.67.22	Remote	192.165.67.22 🇮🇹	1 day, 2 hours, 4 min, 30 sec	34971 ↗	Sent	0 bps	7.81 GB
78.47.50.132	Remote	78.47.50.132 🇩🇪	1 day, 2 hours, 4 min, 48 sec	24940 ↗	Sent	879.93 bps	7.18 GB
62.149.189.11	Remote	62.149.189.11 🇮🇹	1 day, 2 hours, 4 min, 35 sec	31034 ↗	Sent	0 bps	1.44 GB
192.12.192.242	Local	whois.nic.it 🇮🇹	1 day, 2 hours, 4 min, 49 sec	2597 ↗	Rcvd	84.86 Kbit	964.02 MB
224.0.0.18	Remote	vrrp.mcast.net	1 day, 2 hours, 4 min, 49 sec		Rcvd	8.81 Kbit	120.35 MB
213.154.243.80	Remote	213.154.243.80 🇳🇱	18 hours, 57 min, 57 sec	12859 ↗	Sent	4.51 Kbit	116.72 MB

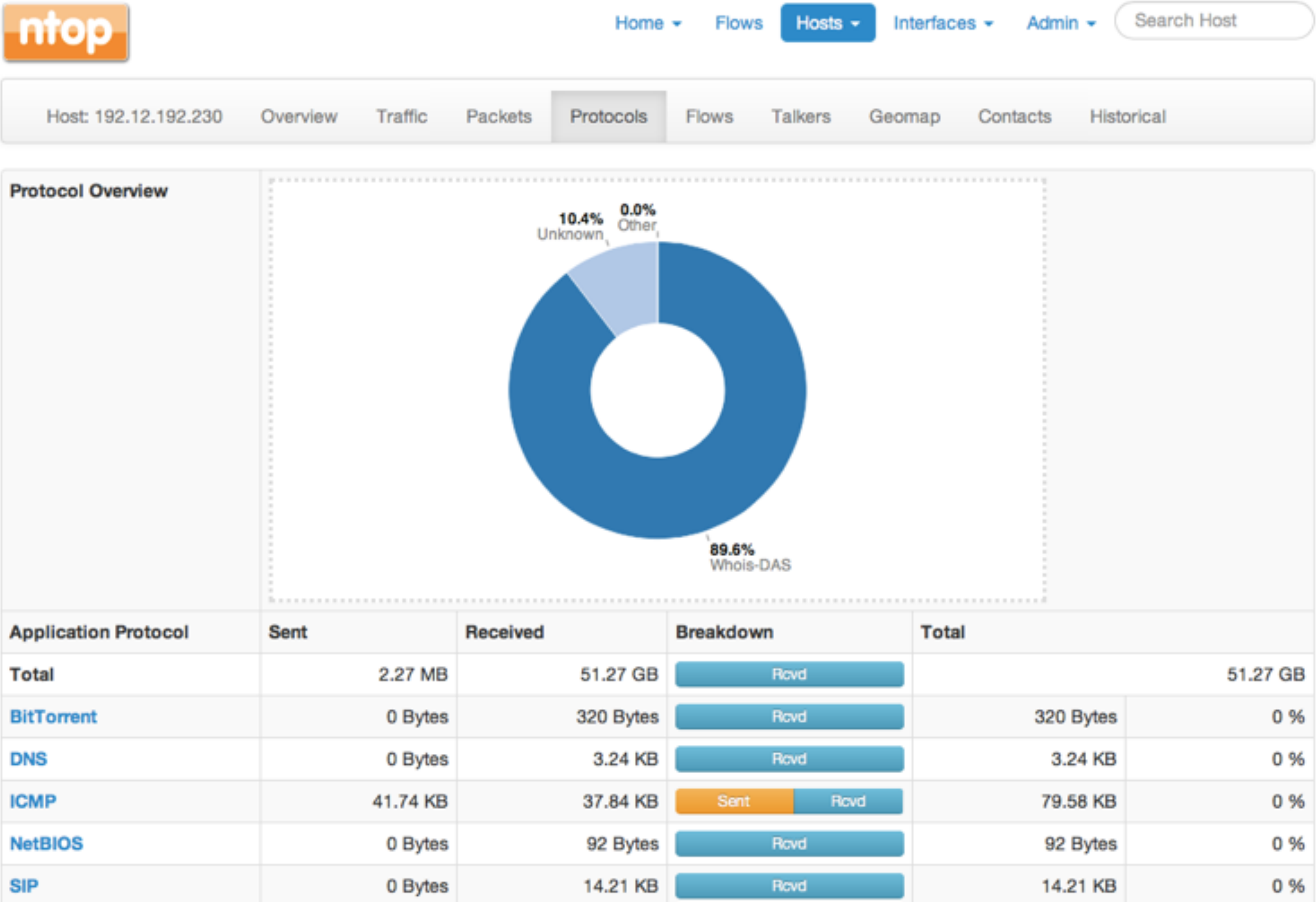
Showing 1 to 10 of 1275 rows

Host Monitoring [2/3]



(Router) MAC Address	00:1B:21:30:81:D0
IP Address	192.12.192.230
ASN	2597 [Registry of ccTLD it - IIT-CNR]
Name	das.nic.it Local
First Seen	10/10/2013 11:47:36 [1 day, 2 hours, 5 min, 14 sec ago]
Last Seen	11/10/2013 13:52:48 [2 sec ago]
Sent vs Received Traffic Breakdown	Rcvd
Traffic Sent	39,290 Pkts / 2.27 MB —
Traffic Received	746,704,852 Pkts / 51.27 GB ↑
JSON	Download
Activity Map	

Host Monitoring [3/3]



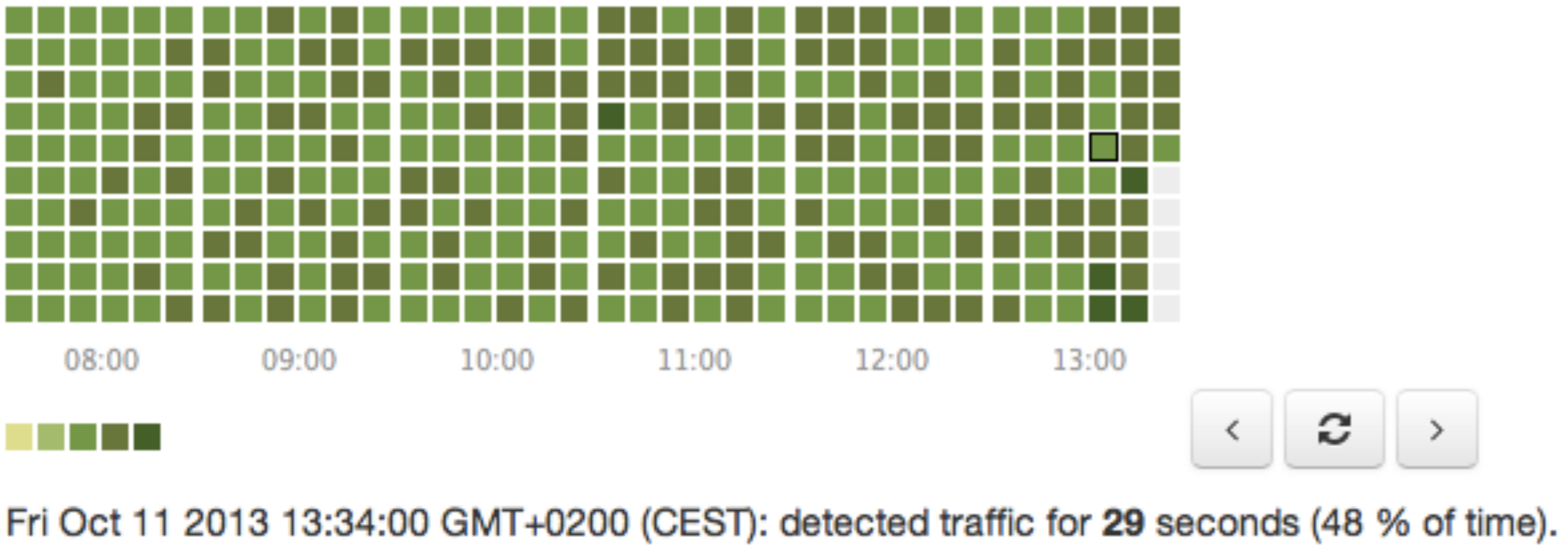
Application Protocol	Sent	Received	Breakdown	Total	
Total	2.27 MB	51.27 GB	Rcvd	51.27 GB	
BitTorrent	0 Bytes	320 Bytes	Rcvd	320 Bytes	0 %
DNS	0 Bytes	3.24 KB	Rcvd	3.24 KB	0 %
ICMP	41.74 KB	37.84 KB	Sent Rcvd	79.58 KB	0 %
NetBIOS	0 Bytes	92 Bytes	Rcvd	92 Bytes	0 %
SIP	0 Bytes	14.21 KB	Rcvd	14.21 KB	0 %

Activity Map

- 1 second resolution host and aggregation activity
- Compressed bitmap

```
> ls -l client14.dropbox.com
4 -rw-rw-rw- 1 nobody nogroup 24 Oct 11 02:31 client14.dropbox.com
```

- Saved persistently on disk (Local Hosts only)

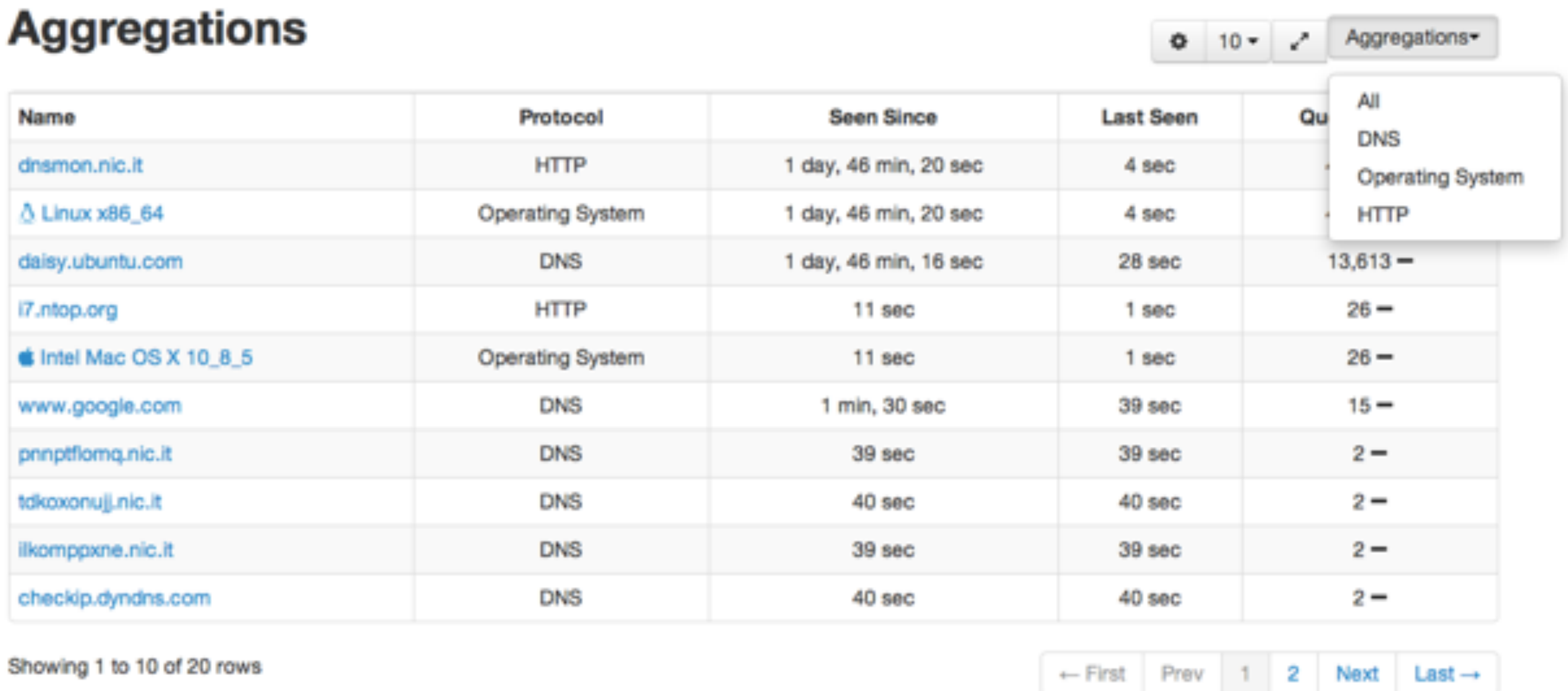


Fri Oct 11 2013 13:34:00 GMT+0200 (CEST): detected traffic for **29** seconds (48 % of time).

Traffic Aggregations [1/2]

- nDPI extracts specific attributes from traffic that ntopng aggregates (if configured):
  - DNS/Whois responses
  - HTTP host names
  - Operating System (from HTTP headers)
- Aggregations can be enabled (they are off by default) and are handled just as flows and hosts.

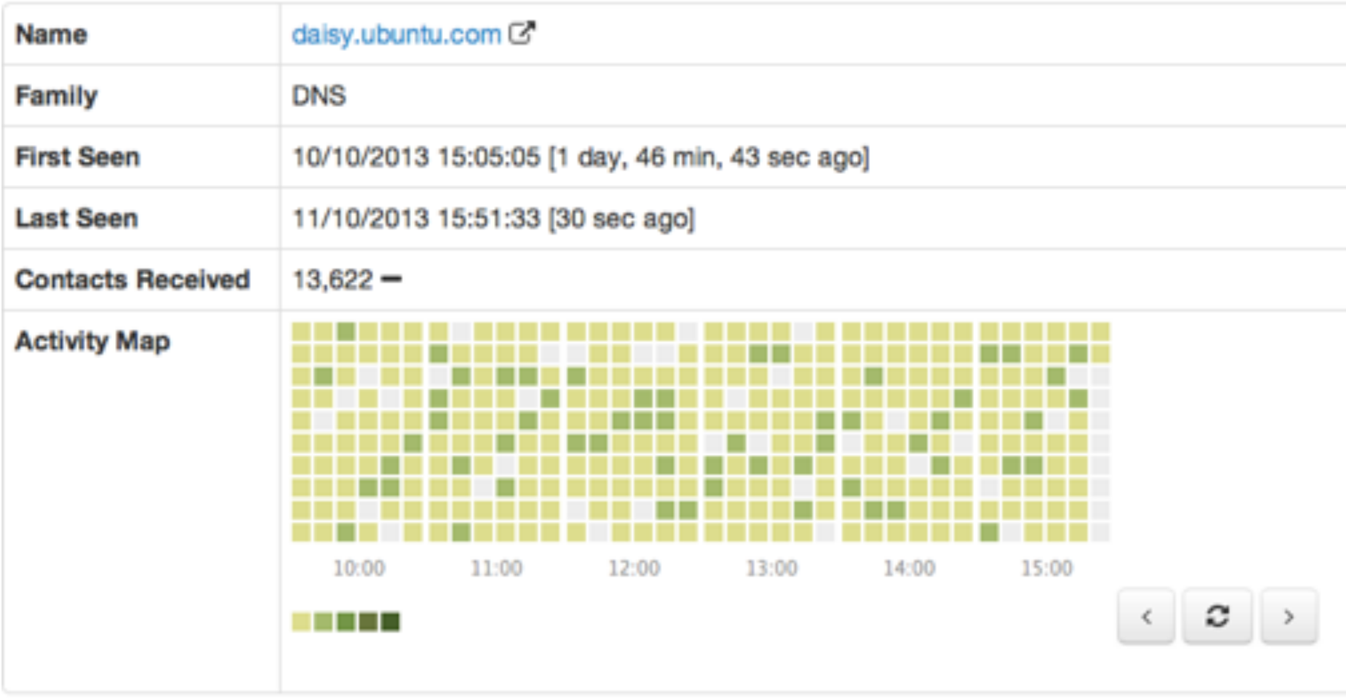
Traffic Aggregations [2/2]



Aggregations

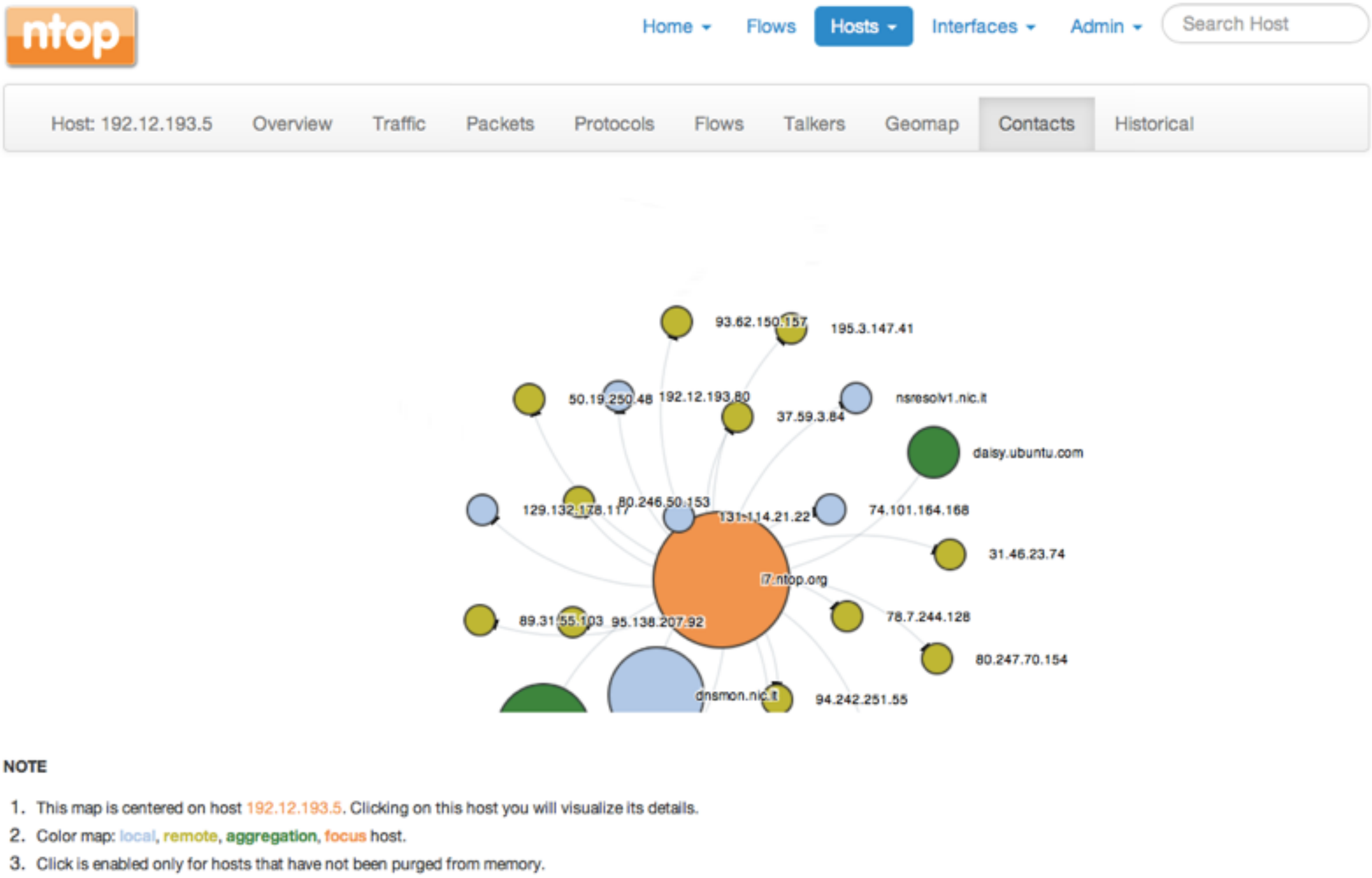
Name	Protocol	Seen Since	Last Seen	Qu
dnsmon.nic.it	HTTP	1 day, 46 min, 20 sec	4 sec	
Linux x86_64	Operating System	1 day, 46 min, 20 sec	4 sec	
daisy.ubuntu.com	DNS	1 day, 46 min, 16 sec	28 sec	13,613 —
i7.ntop.org	HTTP	11 sec	1 sec	26 —
Intel Mac OS X 10_8_5	Operating System	11 sec	1 sec	26 —
www.google.com	DNS	1 min, 30 sec	39 sec	15 —
pnnptflomq.nic.it	DNS	39 sec	39 sec	2 —
tdkoxonujj.nic.it	DNS	40 sec	40 sec	2 —
ilkomppxne.nic.it	DNS	39 sec	39 sec	2 —
checkip.dyndns.com	DNS	40 sec	40 sec	2 —

Showing 1 to 10 of 20 rows



Name	daisy.ubuntu.com
Family	DNS
First Seen	10/10/2013 15:05:05 [1 day, 46 min, 43 sec ago]
Last Seen	11/10/2013 15:51:33 [30 sec ago]
Contacts Received	13,622 —
Activity Map	

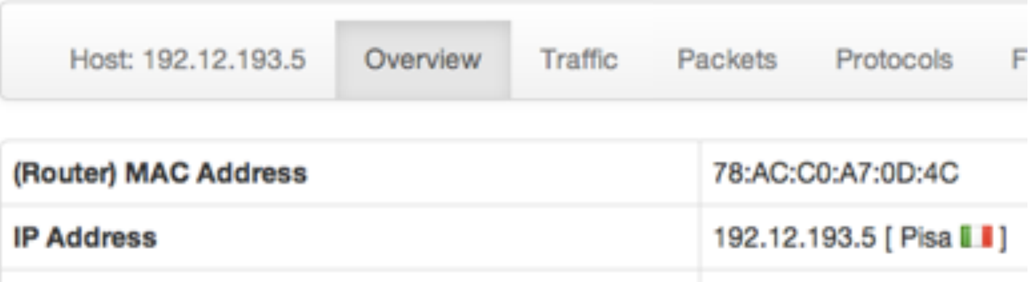
Hosts and Aggregations Interaction



NOTE

1. This map is centered on host 192.12.193.5. Clicking on this host you will visualize its details.
2. Color map: local, remote, aggregation, focus host.
3. Click is enabled only for hosts that have not been purged from memory.

Geolocation



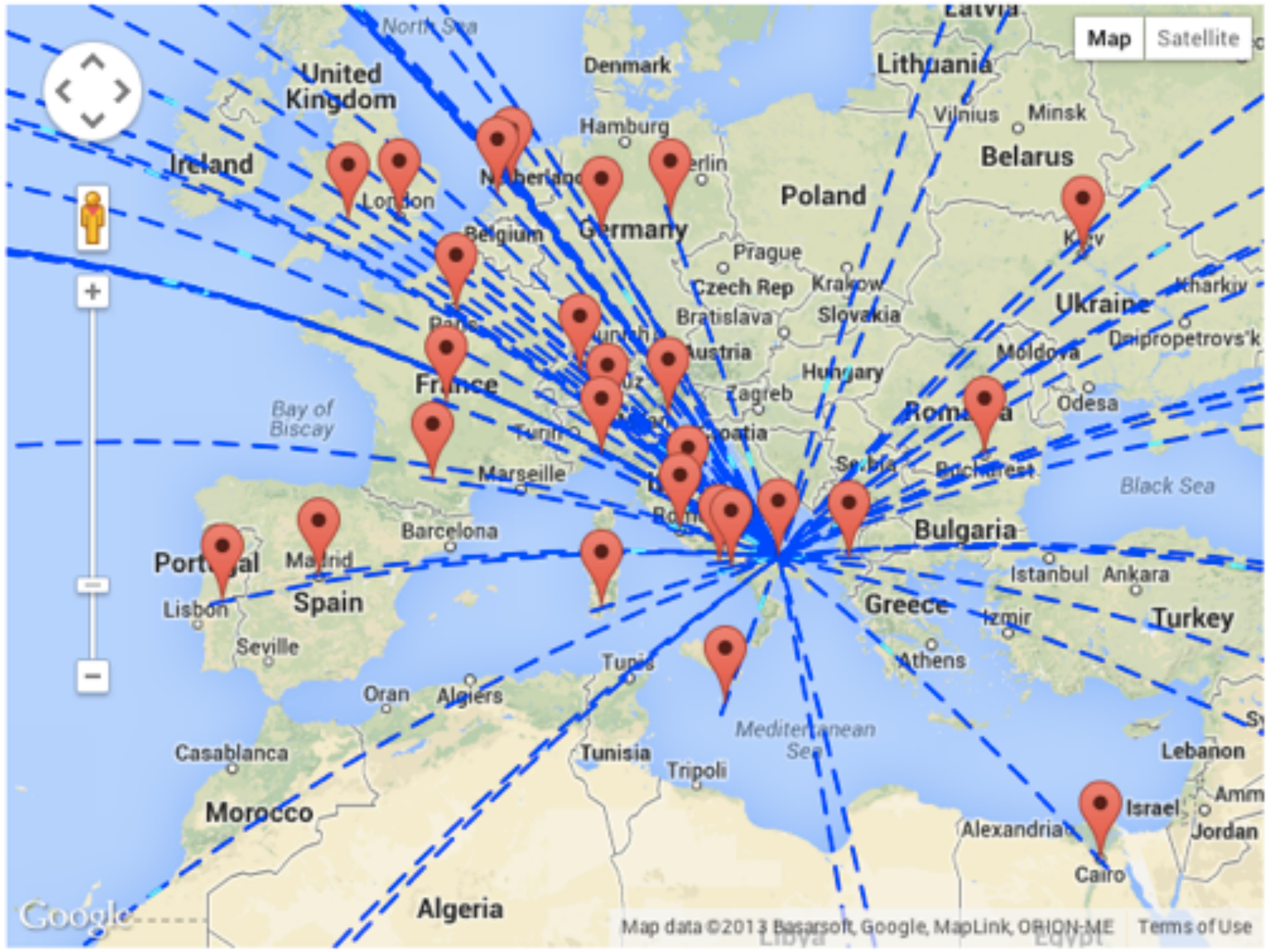
Host: 192.12.193.5	Overview	Traffic	Packets	Protocols	F

(Router) MAC Address	78:AC:C0:A7:0D:4C
IP Address	192.12.193.5 [Pisa 🇮🇹]

Maxmind GeoIP

Map Centered Using HTML 5 Geolocation

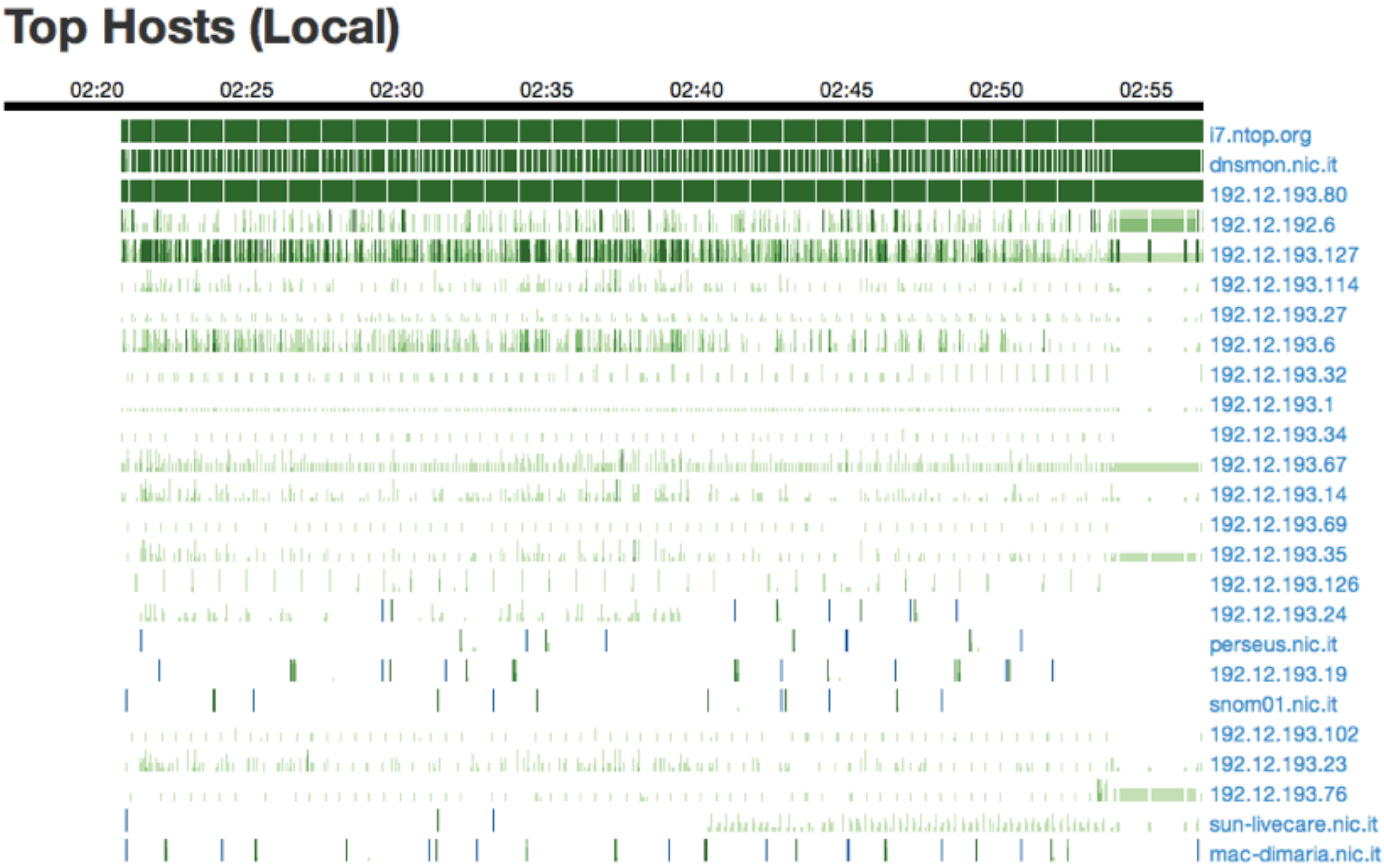
Hosts GeoMap



NOTE

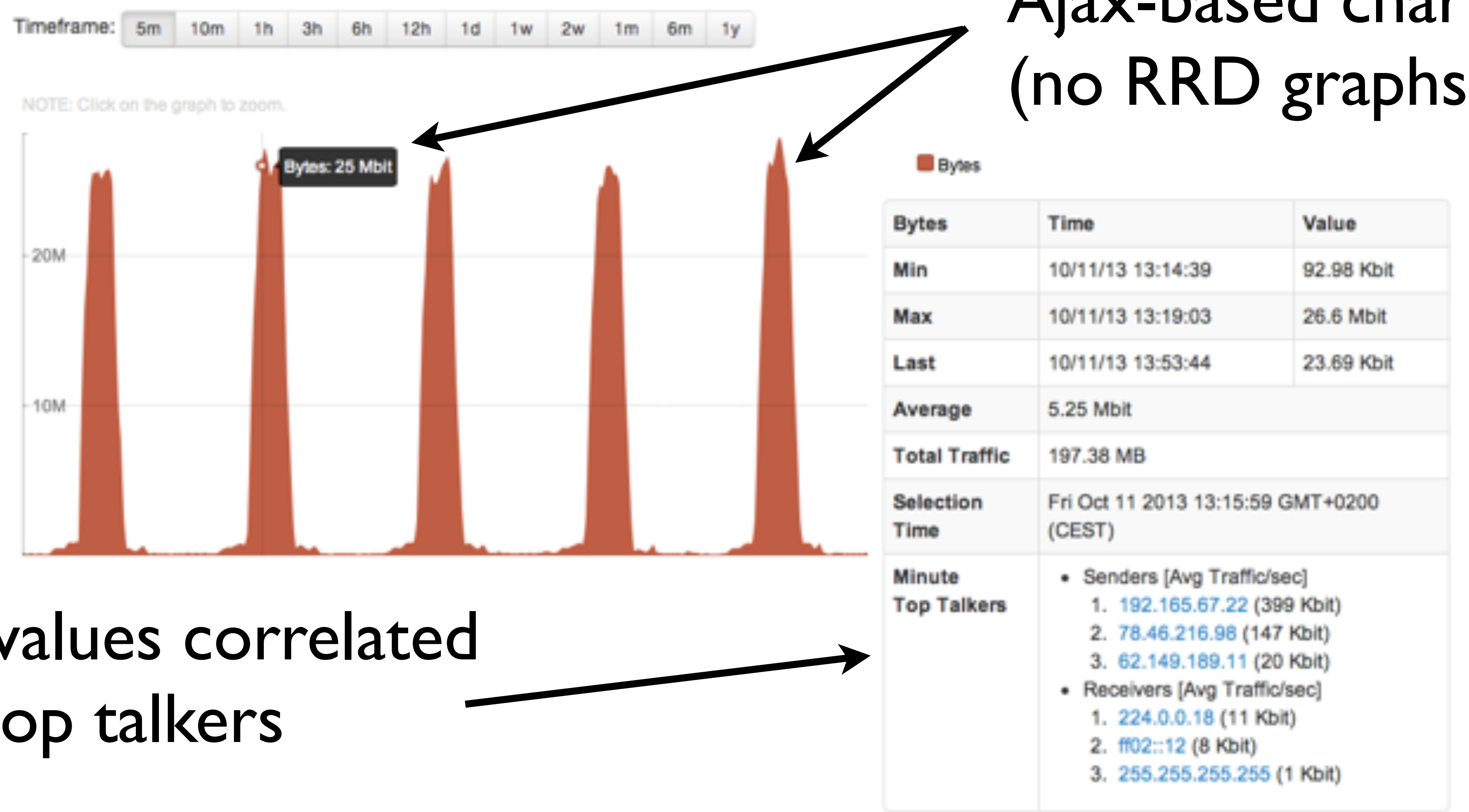
1. Browser reported home map location [Latitude: 43.71949459086955, Longitude: 10.4219399273913]
2. In order to visualize maps you must:
   1. Have a working Internet connection.
   2. Have compiled ntopng with geolocation and started with it.
   3. Have active flows between peers with public IP addresses.
3. HTML browser geolocation is used to place on map hosts based on unknown locations.

Live Host Activities



Historical Activities

- All relevant counters are saved on disk in RRD.
- Interface counters are saved with 1 second resolution. Hosts counters every 5 minutes.



Timeframe: 5m 10m 1h 3h 6h 12h 1d 1w 2w 1m 6m 1y
NOTE: Click on the graph to zoom.
Bytes: 25 Mbit
20M
10M
Bytes

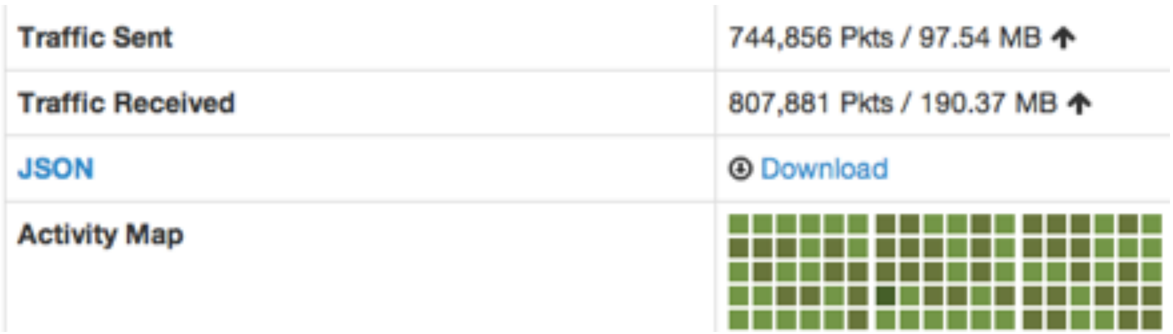
Bytes	Time	Value
Min	10/11/13 13:14:39	92.98 Kbit
Max	10/11/13 13:19:03	26.6 Mbit
Last	10/11/13 13:53:44	23.69 Kbit
Average	5.25 Mbit	
Total Traffic	197.38 MB	
Selection Time	Fri Oct 11 2013 13:15:59 GMT+0200 (CEST)	
Minute Top Talkers	• Senders [Avg Traffic/sec] 1. 192.165.67.22 (399 Kbit) 2. 78.46.216.98 (147 Kbit) 3. 62.149.189.11 (20 Kbit) • Receivers [Avg Traffic/sec] 1. 224.0.0.18 (11 Kbit) 2. ff02::12 (8 Kbit) 3. 255.255.255.255 (1 Kbit)	

Ajax-based charts (no RRD graphs)

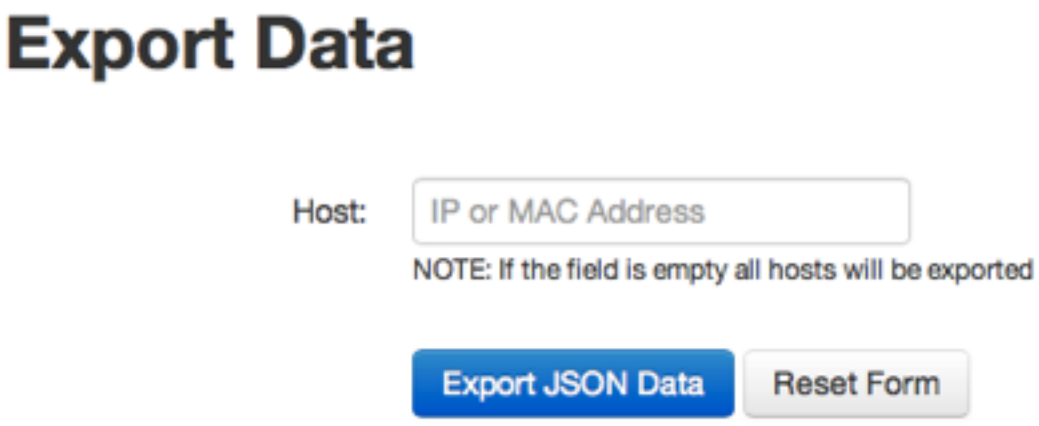
RRD values correlated with top talkers

Using ntopng as a Live Data Source

- ntopng is a server able to serve data to third party applications via HTTP.
- Data is exported via JSON.
- This mechanism can be extended via Lua scripts.



Traffic Sent	744,856 Pkts / 97.54 MB ↑
Traffic Received	807,881 Pkts / 190.37 MB ↑
JSON	Download
Activity Map	



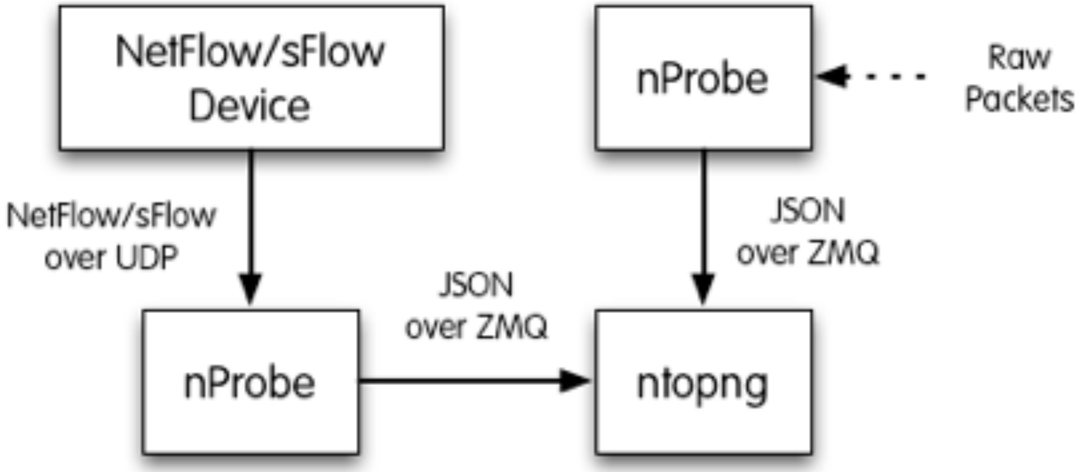
Export Data

Host: IP or MAC Address

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

Using ntopng with NetFlow/sFlow

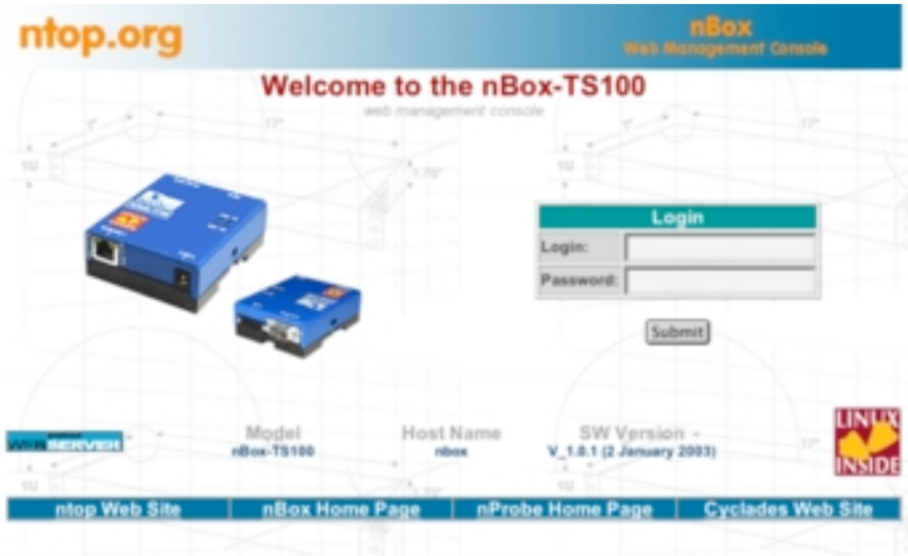
- ntopng can handle flows (Net/sFlow) via nProbe.



- Data Collector (ntopng)
  - `ntopng -i tcp://127.0.0.1:5556`
- Probe (nProbe)
  - `nprobe --zmq "tcp://*:5556" -i eth1 -n none` (probe mode)
  - `nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 2055` (sFlow/NetFlow collector mode)

Embedding ntopng [1/2]

- Historically we have started our first embed attempt in 2003 with the Cyclades TS100.
- The nBox was used to analyse traffic then sent to ntop for representation.
- After 10 years we tried again with ntopng.



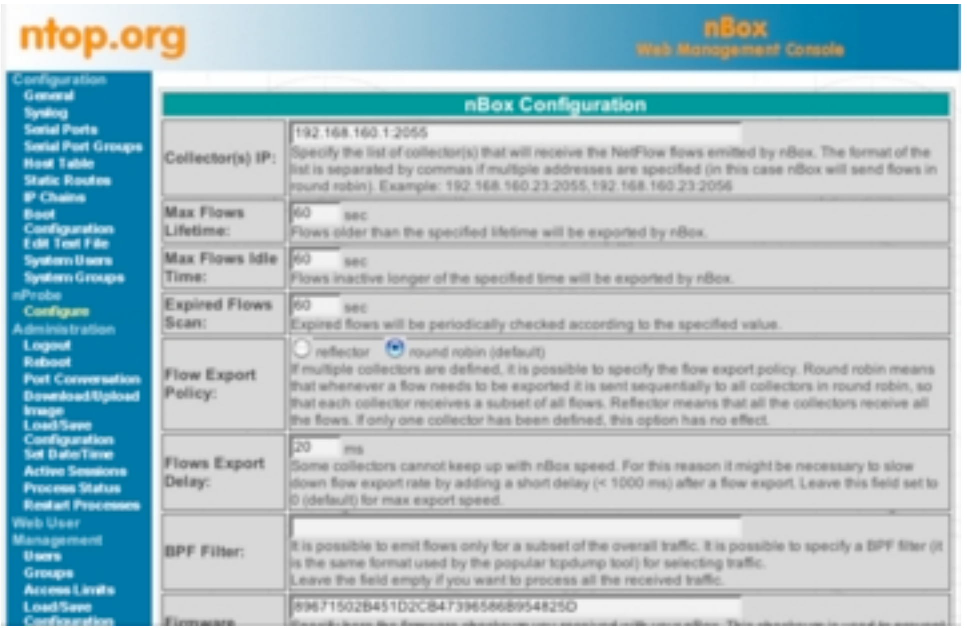
Welcome to the nBox-TS100

web management console

Model: nBox-TS100

Host Name: nbox

SW Version - V_1.0.1 (2 January 2003)



nBox Configuration

Collector(s) IP: 192.168.160.1:2055
Specify the list of collector(s) that will receive the NetFlow flows emitted by nBox. The format of the list is separated by commas if multiple addresses are specified (in this case nBox will send flows in round robin). Example: 192.168.160.23:2055,192.168.160.23:2056

Max Flows Lifetime: 60 sec
Flows older than the specified lifetime will be exported by nBox.

Max Flows Idle Time: 60 sec
Flows inactive longer of the specified time will be exported by nBox.

Expired Flows Scan: 60 sec
Expired flows will be periodically checked according to the specified value.

Flow Export Policy: ○ reflector ● round robin (default)
If multiple collectors are defined, it is possible to specify the flow export policy. Round robin means that whenever a flow needs to be exported it is sent sequentially to all collectors in round robin, so that each collector receives a subset of all flows. Reflector means that all the collectors receive all the flows. If only one collector has been defined, this option has no effect.

Flows Export Delay: 20 ms
Some collectors cannot keep up with nBox speed. For this reason it might be necessary to slow down flow export rate by adding a short delay (< 1000 ms) after a flow export. Leave this field set to 0 (default) for max export speed.

BPF Filter:
It is possible to emit flows only for a subset of the overall traffic. It is possible to specify a BPF filter (it is the same format used by the popular tcpdump tool) for selecting traffic.
Leave the field empty if you want to process all the received traffic.

Firmware: 89671502B451D2CB4739658689548250

Embedding ntopng [2/2]

- The ntopng code compiles smoothly for cheap (36 Euro) boxes such as the BeagleBone Black.
- You can now create your personal/cheap traffic analyser without having to use a PC.
- Post 1.1 release we will optimise support for these devices (cloud).

Final Remarks

- Over the past 15 years ntop created a software framework for efficiently monitoring traffic.
- “We have a story to tell you, not just hacks”.
- Commodity hardware, with adequate software, can now match the performance and flexibility that markets require. With the freedom of open source.
- Available under GNU GPLv3 from http://www.ntop.org/.