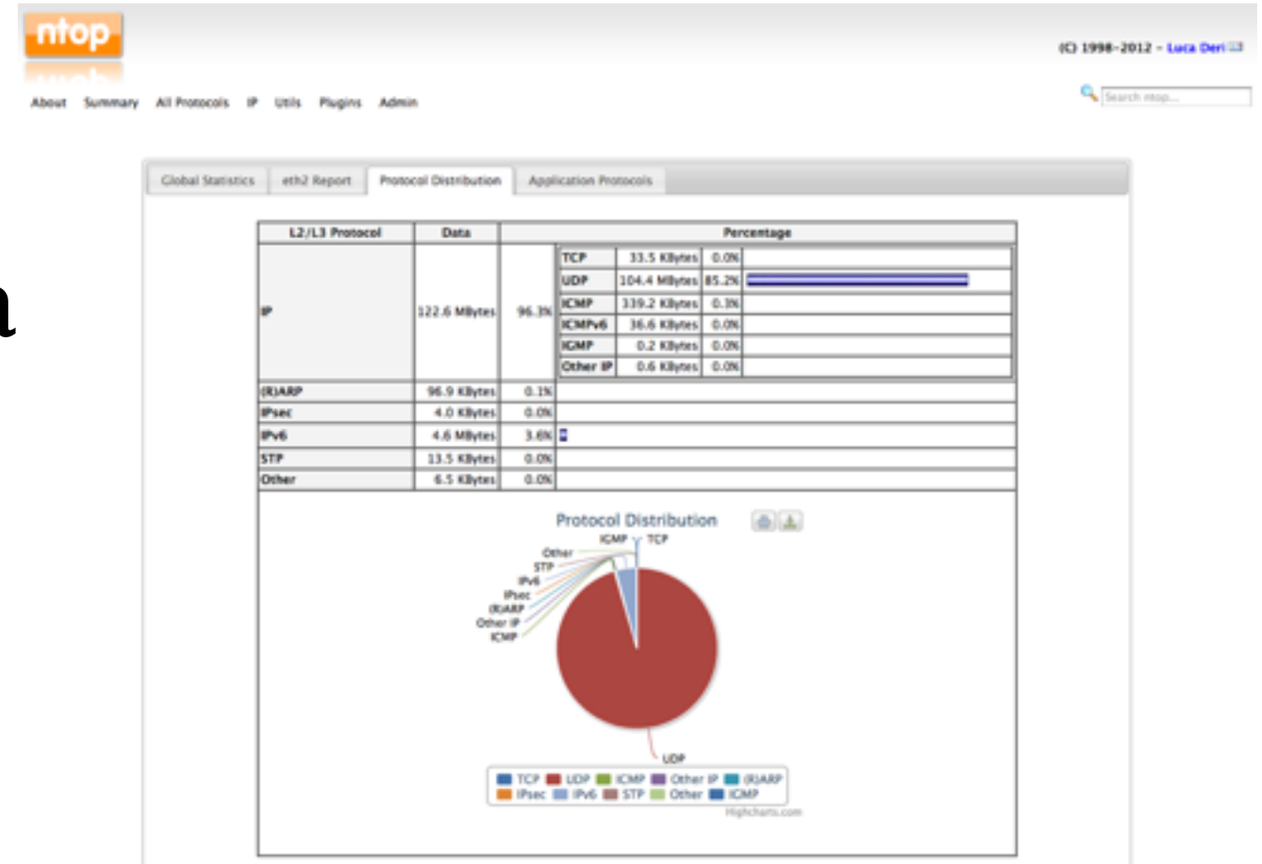
ntop: Monitoraggio di Rete Open Source

Open Source Conference 2013

Luca Deri <deri@ntop.org>

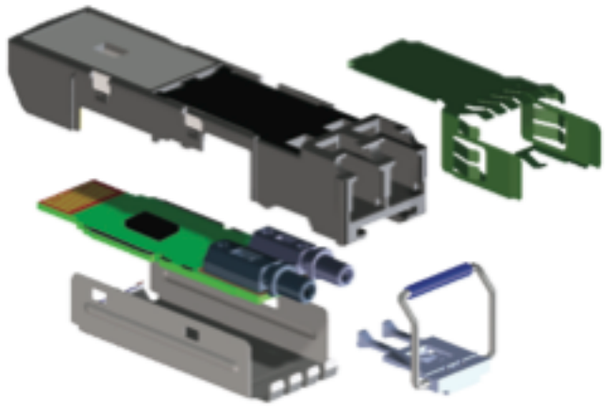
Cosa fa ntop ? [1/3]

- Ditta che opera nel settore del monitoraggio di rete utilizzando strumenti open-source sviluppati nel corso degli anni.
- ntop è stata la prima applicazione rilasciata (1998) finalizzata al web-based network monitoring.



Cosa fa ntop ? [2/3]

- Il nostro software è presente in molti prodotti commerciali...



Integrated ASIC with JDSU technology

Cosa fa ntop ? [3/3]

- ...e vi permettiamo di inviare/ricevere traffico a 1/10 Gbit (any packet size) senza perdita utilizzando schede di rete commerciali.
- Quindi non acceleriamo solo le nostre applicazioni ma anche molte di terze parti.

Obiettivi di ntop

- Produrre soluzioni per il monitoraggio di rete a basso costo che permettono agli utenti di migliorare la loro visibilità di rete.
- Estendere le metriche standard (es. pacchetti, bytes) analizzando in dettaglio i protocolli maggiormente utilizzati in rete (es. email, VoIP, Citrix/RDC).
- Promuovere l'uso del software open-source "Made in Italy" nel campo del monitoraggio di rete.

L'uso del DPI nel Monitoraggio

- Limitare l'analisi del traffico di rete alle intestazioni dei pacchetti non è più sufficiente (né una buona idea perché può trarci in inganno).
- Gli amministratori di rete vogliono conoscere il vero protocollo senza conoscere la porta effettivamente utilizzata.
- Alcuni protocolli (es. HTTP) possono essere analizzati in dettaglio per raccogliere metadati (es. User-Agent) utili per ricavare informazioni ulteriori (es. sistema operativo).

Introduzione a nDPI

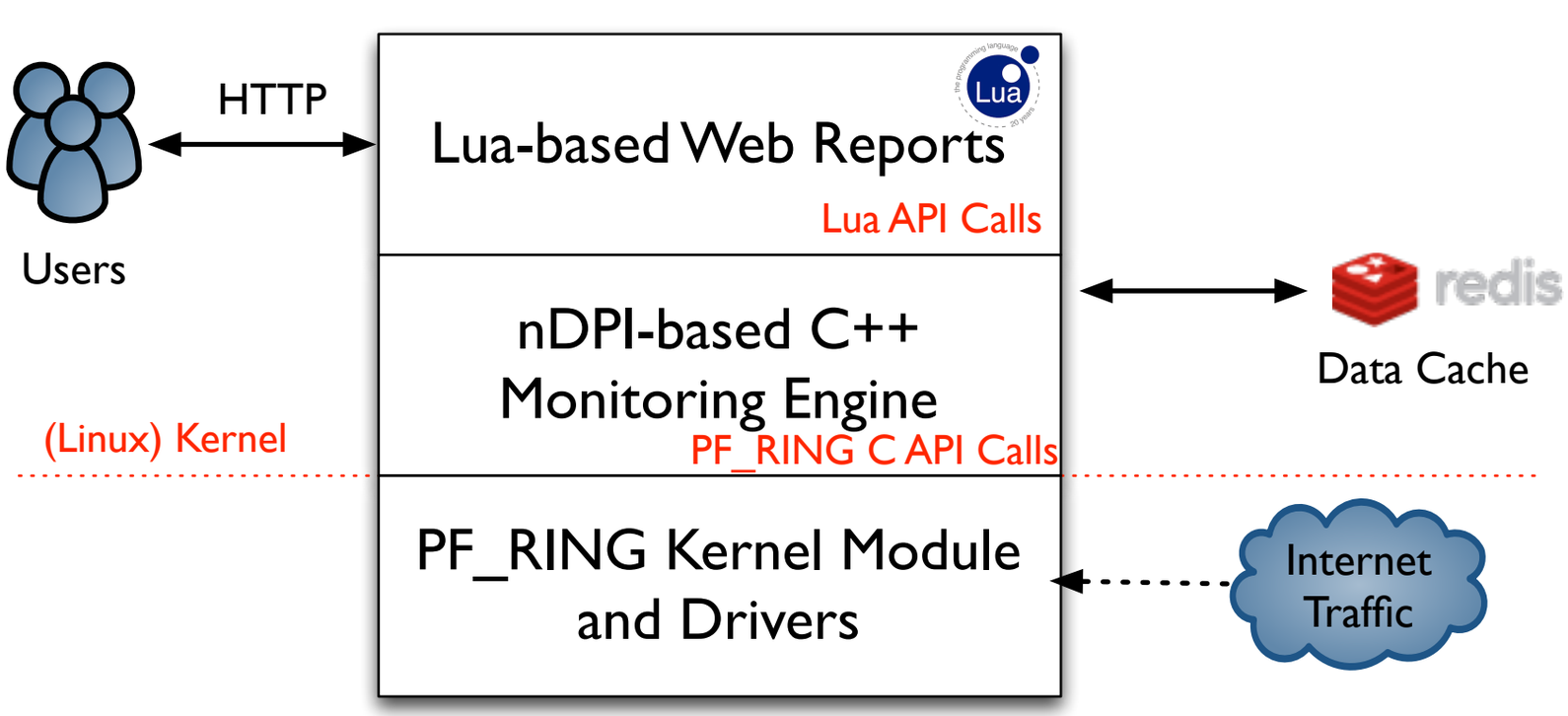
- ntop ha deciso di sviluppare il suo toolkit di DPI chiamato nDPI, in modo da avere una libreria GPL DPI che possa essere usata sia nelle applicazioni di ntop che in quelle di terze parti senza costi aggiuntivi per l'utente finale.
- I protocolli attualmente supportati (~170) includono:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix, Spotify)
  - Business (VNC, RDP, Citrix, *SQL)

Obiettivi di ntopng

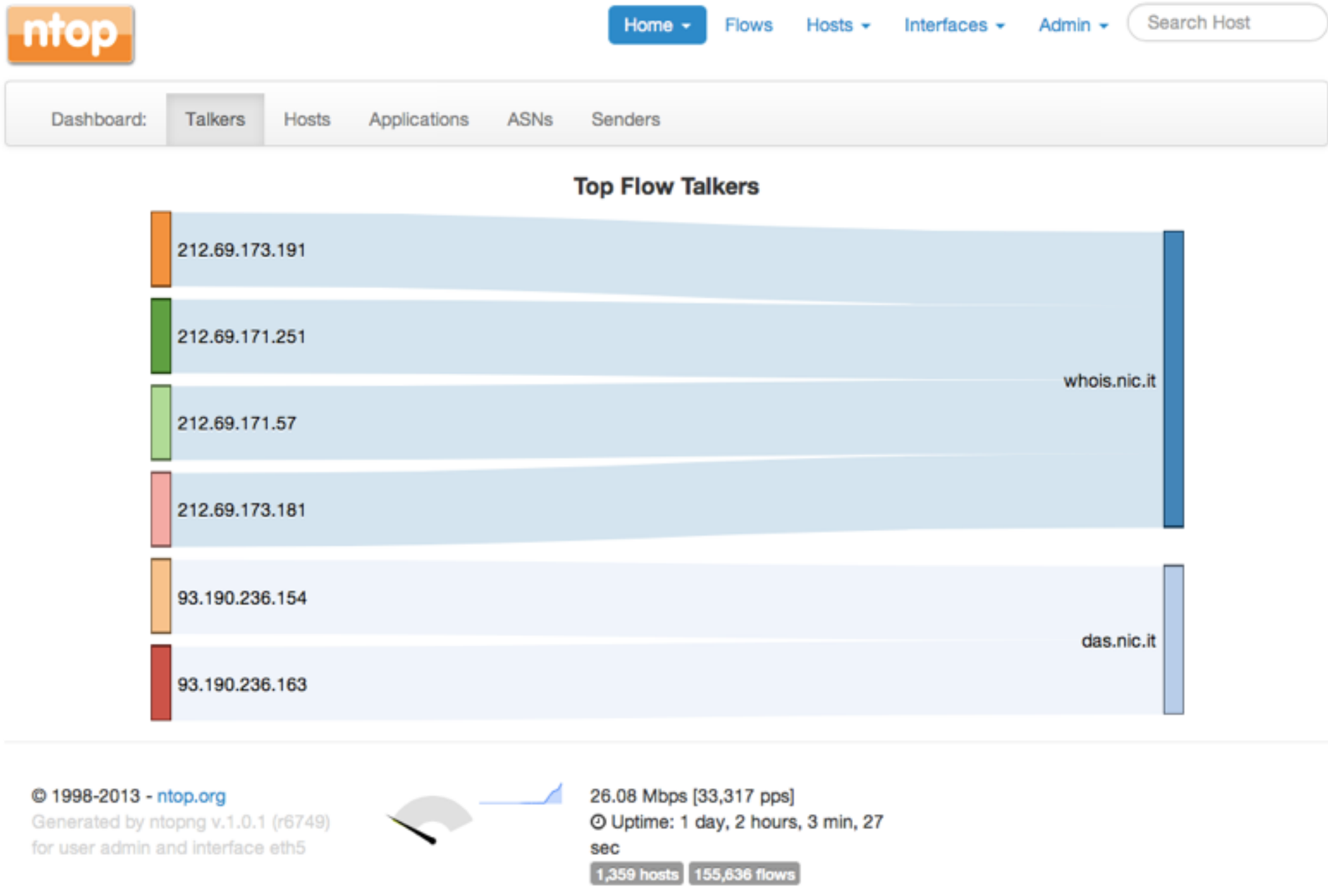
- Monitoraggio in tempo reale del traffico di rete utilizzando una GUI dinamica scritta in HTML 5.
- Tutte le metriche hanno una risoluzione "sub-second" senza aggregare i dati a 5 minuti (SNMP) o alla durata dei flussi (NetFlow/IPFIX).
- Aggregazione in realtime dei dati secondo vari criteri (es. host, sistema operativo, protocollo) per visualizzare gli stessi dati con viste diverse senza appoggiarsi su un backend di databases.

Architettura di ntopng

- ntopng è la console web per il monitoraggio del traffico di rete.
- La sua architettura è divisa in tre livelli distinti:



ntop Dashboard

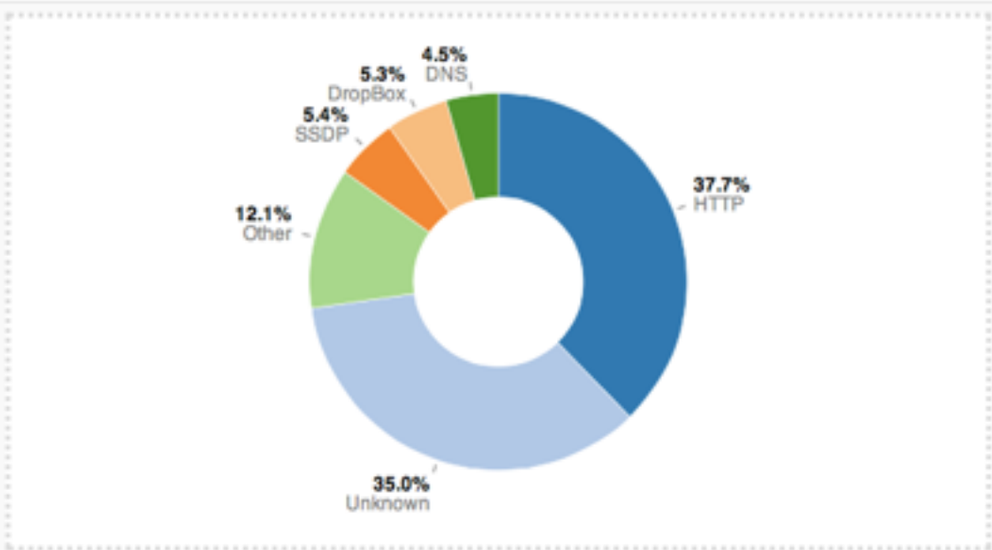


Realtime Reports in ntopng

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

Protocol Overview



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

ntopng come Live Data Source

- In ntopng tutti i dati sono esportabili in JSON.
- ntopng può quindi essere utilizzato come una sorgente di dati per applicazioni di terze parti come Würth-Phoenix NetEye, Nagios, Zenoss.

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

Export JSON Data | Reset Form

Aggregazioni Dati in ntopng

Aggregations

10 ▾ Aggregations ▾

- All
- DNS
- Operating System
- HTTP

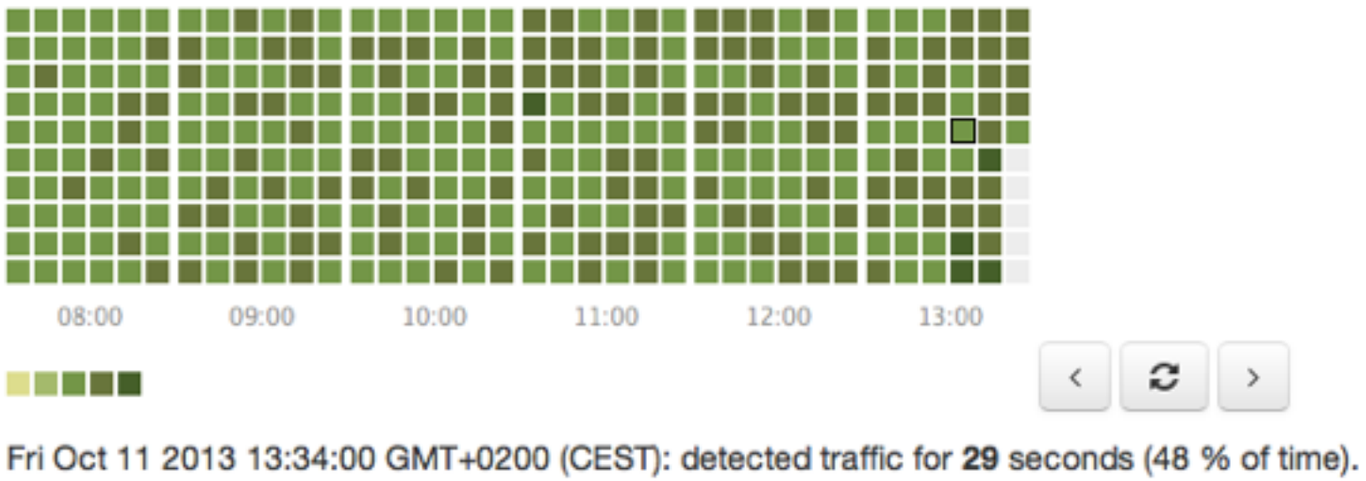
Name	Protocol	Seen Since	Last Seen	Qu
dnsmon.nic.it	HTTP	1 day, 46 min, 20 sec	4 sec	
Linux x86_64	Operating System	1 day, 46 min, 20 sec	4 sec	
daisy.ubuntu.com	DNS	1 day, 46 min, 16 sec	28 sec	13,613
i7.ntop.org	HTTP	11 sec	1 sec	26
Intel Mac OS X 10_8_5	Operating System	11 sec	1 sec	26
www.google.com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

Persistenza dei Contatori di Rete

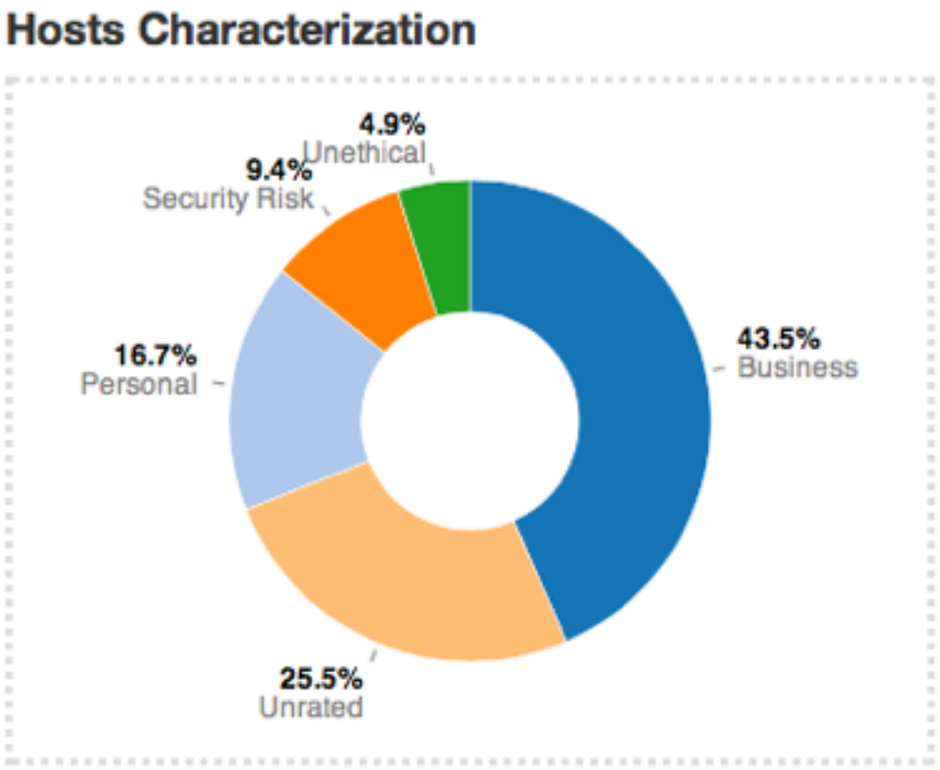
- Tutte le metriche hanno una risoluzione non superiore al secondo.
- I contatori di rete sono salvati come bitmap compresse per avere una vista dettagliata al secondo in poco spazio disco.

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



Categorizzazione del Traffico

- ntopng integra un sistema che categorizza ogni sito Internet indicando la sua tipologia (es. notizie, viaggi, business) sviluppato da blocksi .
- Questo permette di aggregare i dati non in base a siti o indirizzi IP, ma in base alla natura della informazione acceduta.



Conclusioni

- ntopng riesce ad arricchire strumenti di monitoraggio esistenti dando visibilità sul traffico di rete.
- Il prossimo passo è la creazione di sistemi distribuiti a basso costo per monitorare reti distribuite con un approccio cloud-based.

Referenze

- Web Site: http://www.ntop.org
- Blog: http://blog.ntop.org
- Software: http://packages.ntop.org