20 Anni di ntop

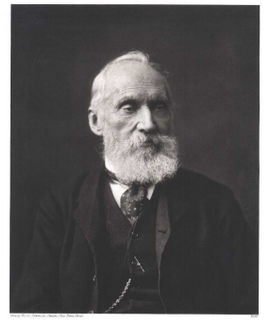
Luca Deri <deri@ntop.org>
@lucaderi

Pisa - 26 Ottobre 2018

Motivazione

If you can't measure it, you can't improve it

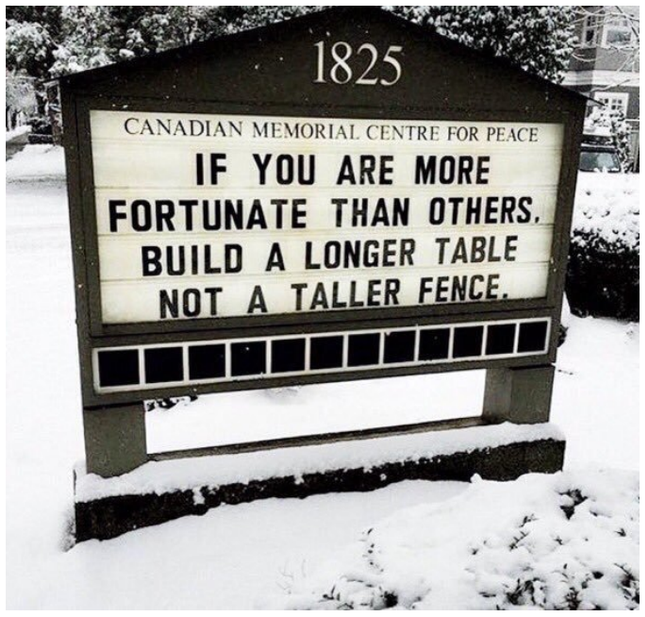
(Lord Kelvin, 1824 – 1907)



Without data, you're just another person with an opinion

(W. Edwards Deming, 1900 - 1993)

ntop: Principi di Base



Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker.

Status in the Hacker Culture

1. Write open-source software
2. Help test and debug open-source software
3. Publish useful information
4. Help keep the infrastructure working
5. Serve the hacker culture itself

How To Become A Hacker, Eric Steven Raymond

1998: Gli Inizi [1/2]

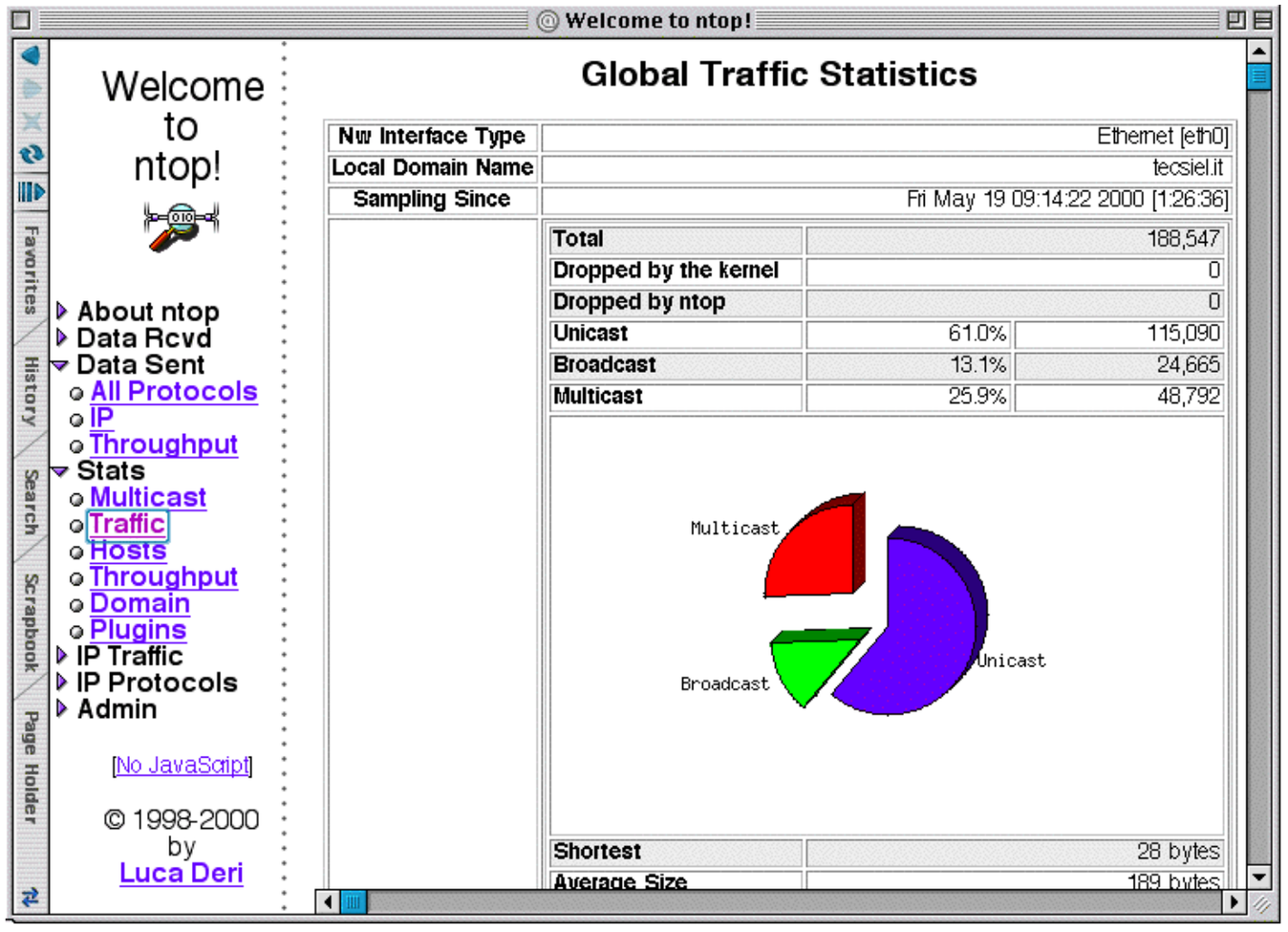
- La rete di unipi era molto limitata a pochi poli ed i servizi offerti erano limitati a mail, web, ftp, gopher, nntp.
- Necessità di capire chi offriva cosa (scan attivo dei servizi offerti), e analizzare quello che passava nel core dalla rete di unipi presso il Centro Serra Servizi Rete Ateneo).
- No mirrors o tap: installare la sonda direttamente sui server che erogavano i servizi di rete.
- Vere soluzioni come HP OV o simili erano costosissime e soprattutto difficili da usare.

1998: Gli Inizi [2/2]

- A quel tempo (e molti esistono ancora oggi) c'erano pochi tool ed estremamente frammentati: uno analizzava l'ARP, l'altro faceva vedere le connessioni….
- Era tempo di scrivere un nuovo tool che in modo "artigianale" facesse cosa serviva: ovvero capire chi si usava la (poca) banda, creava disservizi, ed usava i servizi senza fare il parsing dei file di log dei servizi.
- In sostanza era nato ntop

ntop 1.x [1/2]

- Web-based dal primo giorno, portabile tra Win, Linux e Unix



ntop 1.x [2/2]

	1.1	1.3 [snapshot]
Platforms	• Unix • Win32	
Media	• Loopback • Ethernet • Token Ring • PPP • Raw IP	Added FDDI support
Protocols	• IP • IPX • DecNet • AppleTalk • Netbios • OSI • DLC	
IP Protocols	Fully User Configurable	
Packaging	• Source • Binary • Package	Source

Distributions	• FreeBSD
	• Linux
	  ◦ Debian
	  ◦ Plamo
	  ◦ Suse
	  ◦ Trinux
	  ◦ VA Linux
	  ◦ Caldera
	• Solaris
	• SGI IRIX	

Additional Features	• Network Flows • Local Traffic Analysis • Multithread	• Lightweight Network IDS (Intrusion Detection System) • C++/Perl lightweight API for accessing ntop from remote • Internet Domain Statistics • CGI support • Advanced 'per user' HTTP password protection with encrypted passwords • Support for SQL database for storing persistent traffic information • Remote hosts OS identification (via nmap) • HTTPS (Secure HTTP via OpenSSL) • libwrap support • Virtual/multiple network interfaces support • Graphical Charts (via gdchart) • Perl Interface • WAP support

intop: Per i nostalgici della CLI…

```
                intop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb]     Thpt: 211.9 Kbps/349.7 Kbp
 Host                          Act   -Rcvd-      Sent       TCP       UDP      ICMP
 more                          B   257.4 Kb   281.9 Kb   256.6 Kb       769         0
 zetant                        B   204.2 Kb   232.3 Kb   204.2 Kb         0         0
 tar                           B    42.9 Kb    19.5 Kb    42.9 Kb         0         0
 ibook                         B    32.7 Kb     4.7 Kb    32.7 Kb         0         0
 tecserv                       R        791          0          0       595       196
 bugnoli                       B        602     1.4 Kb          0       602         0
 urano                         B        496     5.1 Kb          0       496         0
 utlrouter                     R         98          0          0         0        98
 mis                           S          0        212          0         0         0
 fiorella                      S          0        486          0         0         0
 piutltst02                    S          0     1.4 Kb          0         0         0
 mostardi                      S          0        952          0         0         0
 193.43.104.55                 S          0        588          0         0         0
 itest1                        S          0        928          0         0         0
 rolly                         S          0         46          0         0         0
 itin2                         S          0         92          0         0         0
 3comhub1                      S          0        610          0         0         0
 re                            S          0     5.6 Kb          0         0         0
 pi100                         S          0     1.2 Kb          0         0         0
 lcardini                      S          0        546          0         0         0
 mbeng                         S          0        602          0         0         0
 itest2                        S          0        600          0         0         0
 fossati-a                     S          0        960          0         0         0
 hpwsutl                       S          0     3.1 Kb          0         0         0
 catlc                         S          0        120          0         0         0
 aut01b                        S          0        243          0         0         0
 biu                           S          0        542          0         0         0
 artico2                       S          0        226          0         0         0
```

```
)3.43.104.154  | 00:50:8B:67:3F:A | COMPAQ COMPUTER CORPORATION
)3.43.104.173  | 00:20:AF:B7:1A:5 | 3COM CORPORATION
)3.43.104.144  | 00:A0:24:EB:35:0 | 3COM CORPORATION
)3.43.104.49   | 00:50:8B:0F:FF:D | COMPAQ COMPUTER CORPORATION
)3.43.104.77   | 00:80:C7:9D:8F:D | XIRCOM
)3.43.104.121  | 00:80:5F:38:AF:D | COMPAQ COMPUTER CORPORATION
)3.43.104.151  | 00:80:5F:C1:7A:8 | COMPAQ COMPUTER CORPORATION
)3.43.104.74   | 00:D0:B7:19:8F:E | INTEL
)3.43.104.91   | 00:00:F8:21:0A:9 | DIGITAL EQUIPMENT CORPORATION
```

```
intop@hme0> uptime
10:36am    up    0 days,  0:10:18,     1 interface

(hme0) -- more.tecsiel.it [193.43.104.10],    213 hosts,    31,815 Pkts / 3.4 MB
intop@hme0> arp -v HEW

| HW Address       | IP Address        | Hostname                    | Vendor
+==================+===================+=============================+==================
| 00:60:B0:68:96   | 193.43.104.13     | tar                         | HEWLETT PACKARD CO.
| 00:60:B0:68:96   | 193.43.104.26     | zen                         | HEWLETT PACKARD CO.
| 00:60:B0:87:8C   | 193.43.104.184    | russo                       | HEWLETT PACKARD CO.
| 00:60:B0:87:8C   | 193.43.104.185    | re                          | HEWLETT PACKARD CO.
| 08:00:09:C2:F2   | 193.43.104.17     | hpwsutl                     | HEWLETT PACKARD
| 08:00:09:5C:6E   | 193.43.104.8      | hpwsric                     | HEWLETT PACKARD
| 08:00:09:D0:D4   | 193.43.104.18     | tecpi2                      | HEWLETT PACKARD

intop@hme0>
```

17.01.2000: Registrato ntop.org [1/2]

- Inizialmente ntop era solo un acronimo.

Luca Deri

University of Pisa
Lungarno Pacinotti 43
56100 Pisa, Italy.
Department: SERRA
Email: deri@ntop.org
Job: Research Scientist and Network Manager.
Goal: Help in making the world a better place (for programmers).
Carry the flame forward!

Welcome and Thanks for visiting my home page.

I was born in 1968. Although I was far too young to remember, the keywords of that year were freedom, equality, free thinking, revolution. In early 70s many free radio stations had birth here in Italy because their young creators wanted to have a way for spreading their thoughts, ideas, emotions and telling the world that they were alive 'n kickin'. The Internet today represents for me what free radios represented in the 70s. This page is here because of my need to tell everybody what I think, do, create. Herein you can find all I've been able to do in the last years that is my humble and tiny contribution to computer science (r)evolution. I was not born in 1968 by coincidence! Thanks for being here.

Teaching Activities

- Corso di Gestione di Rete [Italian]
  1. Programma
  2. Mailing List
  3. Appunti Lezioni [Autore: R. Ferrari]
  4. Lucidi per il corso.
  5. Progetti per l'esame.
- Introduction to Network Management
- Supervisione Tesi
  1. Gaia Maselli
     Riconoscimento di Comportamenti di Rete Inattesi
     Settembre 2001.
  2. Mirko Filoni
     Computing Assets Categorization According to Collected Configuration and Usage Information
     Novembre 2001

Software to Download

- ntop: network top
- SMB_SNMP: SNMP Desktop Based Management
- libpcap for Win32
- Webbin' CMIP

17.01.2000: Registrato ntop.org [2/2]

- Uno dei primi supporter del progetto, registra il dominio e lo "regala" al progetto.
- Questo permette di spostare il tutto da http://jake.unipi.it/~deri/ a www.ntop.org e dare dignità al progetto.

2002: nProbe e sFlow

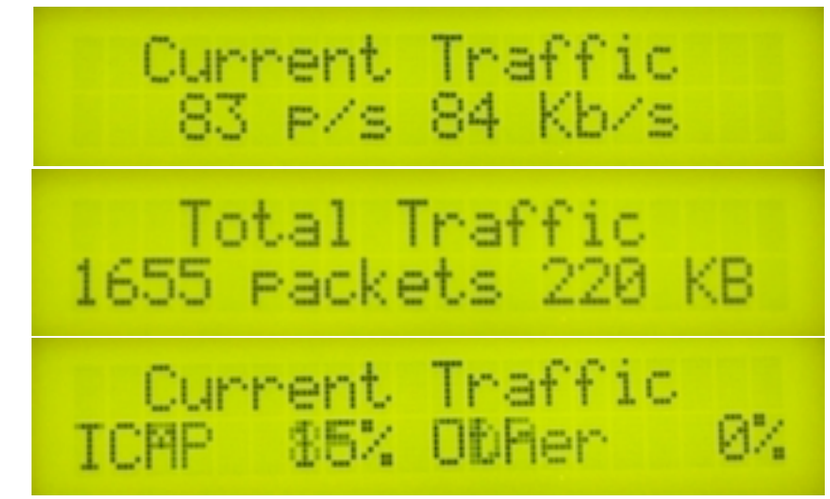
- Open source a volte non è sufficiente, perché ci sono da supportare standard come sFlow/NetFlow: nasce nProbe 1.x/2.x e ntop 2.x

	v. 1.x	v. 2.x
Support for Unix and Win32	Yes	Yes
NetFlow v5 Compliant	Yes	Yes
Multiple Collectors	No	Yes
Reflector Mode	No	Yes
Win32 Service	No	Yes (on NT/2K/XP)
Flexible Logging	No	Yes
Export Flow Delay	No	Yes
Minimum TCP Flow Export	No	Yes
LCD Display Support	No	Yes (Unix only)
Available on Embedded System	No	Yes

2002: I primi nBox

Main Features

- Small NetFlow probe based on nProbe
- Based on a Cyclades TS100 box
- Dual-CPU PowerPC (MPC855T)
- Linux Inside
- Interfaces: 10/100 Ethernet, RS-232, RS-485
- Access via SSH, Telnet, Web (http/https)
- Small form factor (7x8.5x3 cm - 2.8x3.4x1.2 in)
- Robust case with no moving parts
- Boot in less than 30 seconds
- Easy configuration via the Web interface



2003/4: PF_RING

- Con l'aumentare del traffico era chiaro che non si poteva andare molto lontano con Linux che aveva altri obiettivi (generalità vs efficienza).
- Coinvolto nel progetto EU Scampi, è nato PF_RING come risposta alle schede di rete basate su FPGA quali Endace.

Introduction

PF_RING is a new type of network socket that dramatically improves the packet capture speed, and that's characterized by the following properties:

1. Available for Linux kernels 2.4.X and 2.6.X
2. Device driver independent (best results can be achieved using network cards that support NAPI such as the Intel cards)
3. Kernel-based packet capture and sampling.
4. Libpcap support (see below) for seamless integration with existing pcap-based applications.
5. **New** Ability to work in transparent mode (i.e. the packets are also forwarded to upperlinks so existing applications will work as usual).

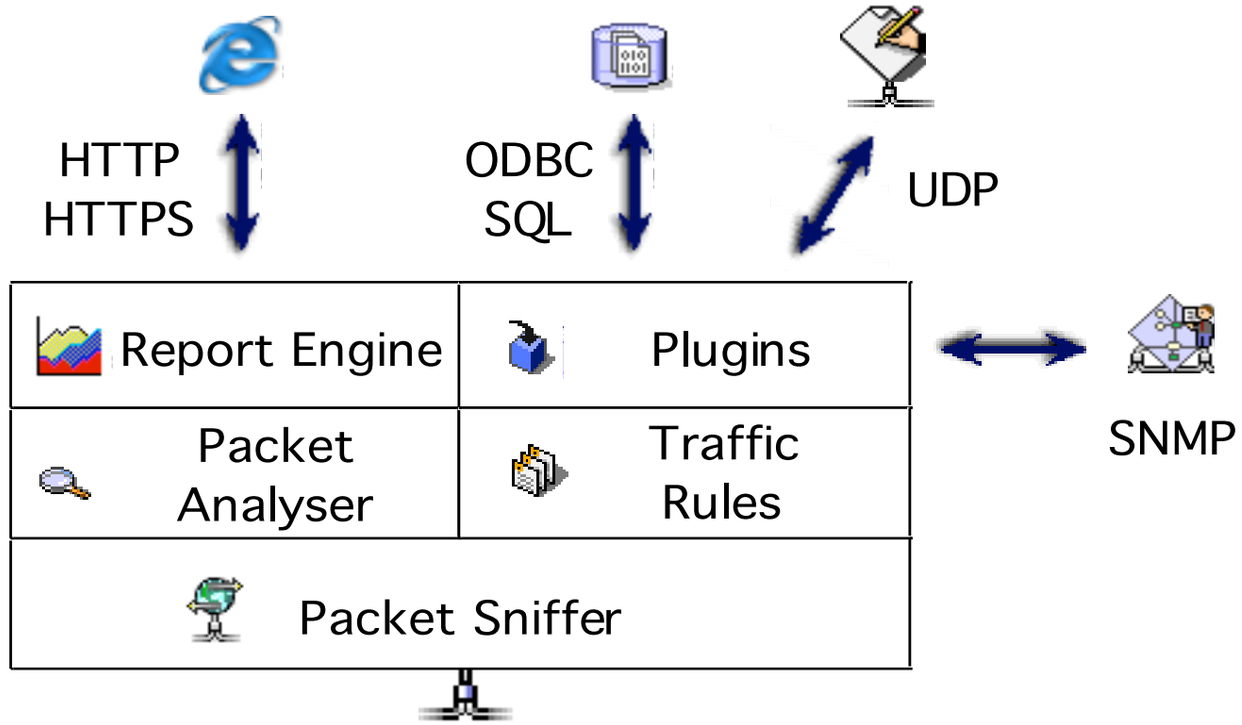
If you want to know about PF_RING internals you have two options. Either read the paper Improving Passive Packet Capture:Beyond Device Polling or have a look at the source code.

2004/8: Consolidamento del Progetto [1/2]

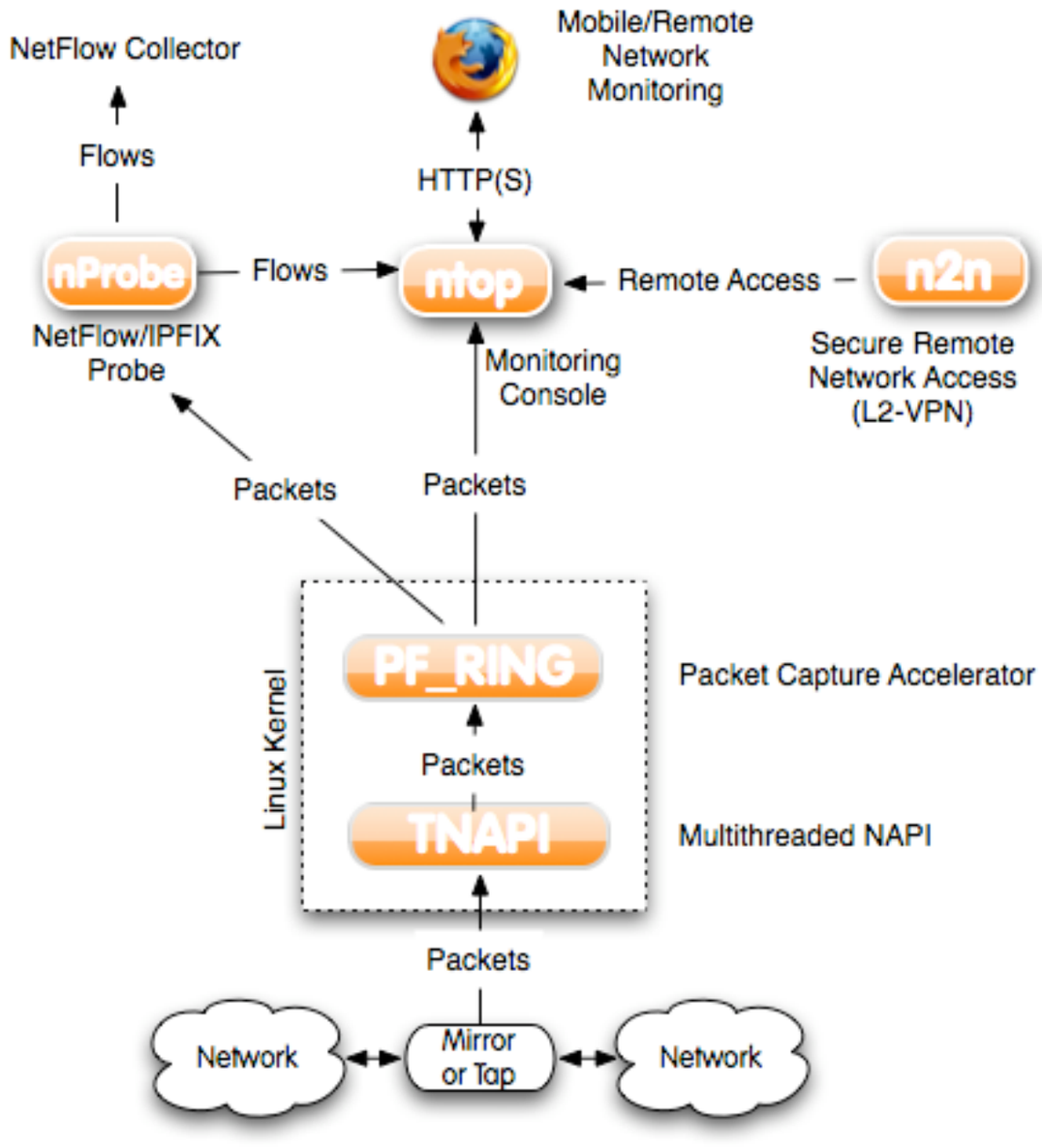
What new with ntop?

June 2nd, 2008	Meet ntop in Bremen at AIMS 2008
May 23rd, 2008	Meet ntop in Athens at the 3rd Open Source Software Conference
Apr 23rd, 2008	Running ntop on 10 Gbit networks using cPacket's cTap [press release]
Apr 9th, 2008	IP Traffic monitoring at 10 Gbit and above
Mar 27th, 2008	n2n: a layer-two peer-to-peer VPN is born: please contribute!
Jul 20th, 2007	svn.ntop.org is born: subversion and track.
June 9th, 2007	ntop 3.3 released: improved stability, ease of use, U3 support and graphical GUI (Win32).
May 24th, 2007	nBox Envision your network with nBox (Embedded Ntop).
Mar 18th, 2007	Use dynamic bloom filtering with PF_RING.
Feb 6th, 2007	ntop 3.3rc seeded 3Com embraces ntop for network traffic monitoring.
July 13th, 2006	Download VMware ntop virtual appliance
June 7th, 2006	Linux magazine inteviews Luca [Italian]
Mar 30th, 2006	wiki.ntop.org is born. Please contribute!
Oct 22nd, 2005	ntop 3.2 is out: VoIP support, NetFlow v9/IPFIX enhancements, performance boost, more statistics and stability.
Aug 26th, 2005	Released nProbe 4.0 an plugin-extensible NetFlow v5/v9/IPFIX flow able to operate at Gigabit speeds and analyze VoIP (Voice over IP) traffic.
May 4-6th, 2005	Meet ntop at the RIPE 50 Meeting in Stockholm
Dec 21st, 2004	ntop 3.1 is out: virtual NetFlow/sFlow interfaces, new appearance, smarter memory usage, iSCSI/FibreChannel support, stability.
Dec 10th, 2004	Released PF_RING 3.0 CVS available.
Apr 23th, 2004	Released PF_RING 2.1: stable, easy to build, new features.
Mar 23rd, 2004	Released ntop 3.0: IPv6, FibreChannel, NetFlow v9, nFlow, XML-export, improved RRD support and much more.
Feb 20th, 2004	Released PF_RING 2.0: how to capture over 550'000 pkt/sec using Linux on your commodity PC.
Jan 12th, 2004	Released nProbe 3.0 a NetFlow v5/v9/nFlow flow able to operate at Gigabit speeds.
Nov 23rd, 2003	Released nBox86: embed ntop and nprobe into your own x86 PC.

2004/8: Consolidamento del Progetto [2/2]



2009: Nascita dell'Ecosistema



2010/11: PF_RING DNA, Blog

HOME | BLOG | PRODUCTS | SOLUTIONS | GET STARTED | SUPPORT | SHOP

Released PF_RING 5.1 and TNAPIv2

on SEPTEMBER 25, 2011

PF_RING 5.1 is a maintenance release that addresses some issues we identified in 5.0 that we released early this month. We have listen to your comments and tried to improve our software applications both in terms of stability and speed.

In this release we introduce (PF_RING 5.0 was lacking TNAPI as we were busy coding [...]

Continue Reading →

Inline Snort Multiprocessing with PF_RING

on SEPTEMBER 23, 2011

Dear all,
our friends at MetaFlows have tested snort on top of PF_RING DAQ using 6765 Emerging Threats Pro rules. Using PF_RING-aware drivers (that are not optimized at all for TX), they have achieved a sustain rate of 700 Mbit in IPS mode. Guess what you can do using DNA.

Continue Reading →

Low RX/TX Latency with DNA

on SEPTEMBER 15, 2011

One of the great consequences of the DNA design, is that user-space applications can now transmit and receive packets without going through the kernel TCP/IP stack at all. This can be profitably used to reduce network latency bypassing the stack, and reading the number of user-space stacks that have been developed in the past years [...]

Continue Reading →

BROWSE BY CATEGORIES

- Announce (9)
- DNA (8)
- nProbe (22)
- ntop (17)
- PF_RING (32)
- TNAPI (10)
- vPF_RING (1)

BROWSE BY DATE

- September 2011 (5)
- August 2011 (3)
- July 2011 (2)
- June 2011 (4)
- May 2011 (6)
- April 2011 (3)
- March 2011 (4)
- February 2011 (5)
- January 2011 (2)
- December 2010 (1)
- November 2010 (4)
- October 2010 (4)
- September 2010 (4)
- August 2010 (1)

2011: Nasce nDPI

nDPI

Open and Extensible LGPLv3 Deep Packet Inspection Library.

nDPI is a ntop-maintained superset of the popular OpenDPI library. Released under the LGPL license, its goal is to extend the original library by adding new protocols that are otherwise available only on the paid version of OpenDPI. In addition to Unix platforms, we also support Windows, in order to provide you a cross-platform DPI experience. Furthermore, we have modified nDPI do be more suitable for traffic monitoring applications, by disabling specific features that slow down the DPI engine while being them un-necessary for network traffic monitoring.

nDPI is used by both ntop and nProbe for adding application-layer detection of protocols, regardless of the port being used. This means that it is possible to both detect known protocols on non-standard ports (e.g. detect http non ports other than 80), and also the opposite (e.g. detect Skype traffic on port 80). This is because nowadays the concept of port=application no longer holds.

2012: 10 Gbit e ntop 5.x

- Grazie alla partnership con Silicom Inc, PF_RING ha accesso a schede a 10 Gbit e viene aggiunto il support a 10 Gbit.
- Nasce PF_RING DNA (successore di nCap), e libzero. 
- Rilascio ntopng 5.x: ultima release, troppi limiti architettura e performance, GUI old fashion, troppi protocolli obsoleti.

2013: Nasce ntopng

ntop is back: ntopng 1.0 just released

on JUNE 30, 2013

After 15 years since the introduction of the original ntop, it was time to start over with a new, modern ntop. We called it ntopng, ntop next generation. The goal of this new application are manyfold:

1. Released under GNU GPL3.
2. Feature a modern, HTML5 and Ajax-based dynamic web interface (caveat: you need a modern browser to use ntopng).
3. Small application engine, memory wise and crash proof.
4. Ability to identify application protocols via nDPI, ntop's open-source DPI (Deep Packet Inspection) framework.
5. User's ability to script, extend, and modify ntopng pages coding them in LuaJIT, a small yet lighting fast language.
6. Characterise HTTP traffic by leveraging on block.si categorisation services. ntopng comes with a licensing key, but you can acquire a private key by contacting info@block.si.
7. Use of redis as data cache, for splitting the ntopng engine from data being saved.
8. Ability to collect flows (sFlow, NetFlow and IPFIX) using nProbe as probe/proxy.
9. Fast, very fast engine able to scale up to 10 Gbit on commodity PCs when using PF_RING/DNA.
10. Support of Unix, BSD, MacOSX and Windows (including 7/8).

Riscritto da zero in meno di 6 mesi, nativamente basato su nDPI, nessuna linea di codice del vecchio ntop é stata riutilizzata nel nuovo ntopng.

2014: PF_RING ZC e Sysdig

- PF_RING DNA viene rimpiazzato da PF_RING ZC che consolida il lavoro fatto in DNA e Libzero.
- Grazie a ZC, n2disk riesce ad operare a 10 Gbit line rate.
- Primi esperimenti con la visibilità di applicazioni e sistema integrando Sysdig con nProbe: interessante ma troppo oneroso in termini di CPU e risorse macchina. Da ripensare.

2015: ntopng 2.x

- Con ntopng 2.x l'ecosistema si è definitivamente aperto alle terze parti come ElasticSearch/Kibana.
- PF_RING 6.x e' diventato la lingua franca dei sistemi di cattura supportando 1/10/40 Gbit ed offrendo in un solo framework supporto per tutti i maggiori costruttori di schede di rete basate su FPGA.

2016: 100 Gbit, nProbe Cento

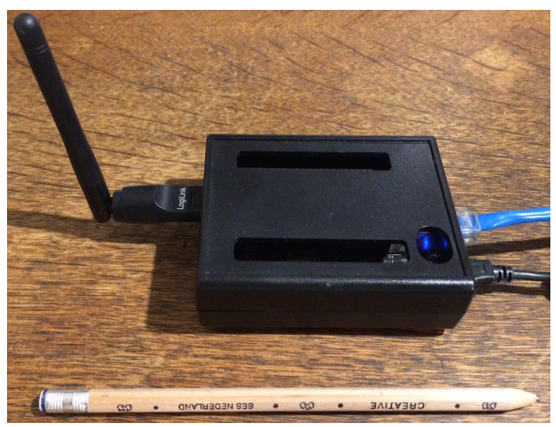
- PF_RING guadagna il supporto al 100 Gbit inizialmente con le schede Napatech e poi Accolade ed Intel RRC.
- Con l'avvento del 100 Gbit va ridisegnato nProbe per farlo scalare di un 10x. Nasce nProbe Cento che permette di monitorare datacenter e 100 Gbit: primo probe (unico?) sul mercato capace di analizzare il traffico a 100 Gbit su un solo server.

2017: ntopng 3.x, nScrub

- Dopo molti mesi di lavoro viene rilasciato ntopng 3.x che consolida un lavoro di pulizia importante di codice e lo rende più versatile ed aperto.
- Introdotti in ntopng i primi algoritmi per poter analizzare il traffico IoT/Fog, e scoprire anomalie nel traffico di rete relative a problemi di cybersecurity.
- Rilascio nScrub per mitigare attacchi DDoS in modalità software pura.

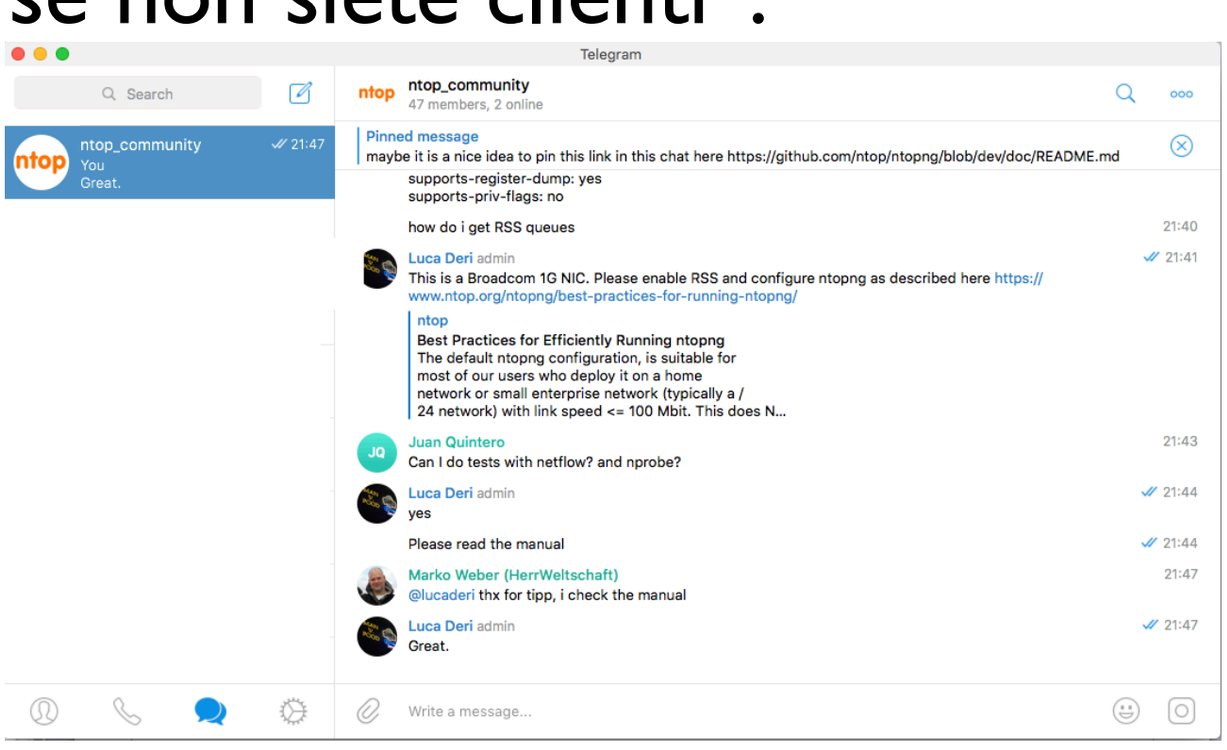
2018: ntopng nEdge

- Abbiamo diviso ntopng in due
  - ntopng (monitoring)
  - nEdge (inline, disegnato per proteggere il network edge)
- Experiments, experiments, experiments…
  - È da tempo che stiamo provando a costruire una device a basso costo capace di proteggere bambini, scuole, reti. Non ci siamo ancora riusciti per i costi hw, ma ce la faremo :-)



ntop: La comunità

- Per molti open-source significa "gratis", ma non è proprio così. Significa
  - Far parte di una comunità: http://t.me/ntop_community (24 x 7 x 365)
  - Ricevere assistenza anche "se non siete clienti": siamo opensource
  - Poter contribuire con codice e fix
  - Influenzare la roadmap, riportare bachi, proporre soluzioni



ntop: I Prossimi Passi

- Organizzare periodicamente eventi itineranti in stile meetup/workshop per riunire la comunità
- Istituire un premio/borsa di studio per studenti che vogliano contribuire allo sviluppo dei nostri tool.
- Trovare un community manager.
- Feedback, segnalazioni e commenti: http://20anni.ntop.org/

E ora un po' di pubblicità