ntop

# Monitoring high-speed networks using ntop

ntop.org

Riccardo Paterna <paterna@ntop.org>

# ntop

## Project History

- Iniziato nel 1997 come monitoring application per l'Università di Pisa
- 1998: Prima release pubblica v 0.4 (GPL2)
- 1999-2002: Registrato ntop.org, creata mailing lists (ntop and ntop-dev) porting su piu piattaforme e distribuzioni Linux .
- 2002-03: Versione 2.x, aggiunto supporto per protocolli commerciali (NetFlow v5 and sFlow v2).
- 2004-05: Version 3.x (molte parti sono state riscritte), aggiunto supporto RRD, IPv6 (Loria) e SCSI/FibreChannel (Cisco), NetFlow V9/IPFIX draft, sFlow v5, VoIP.

# ntop

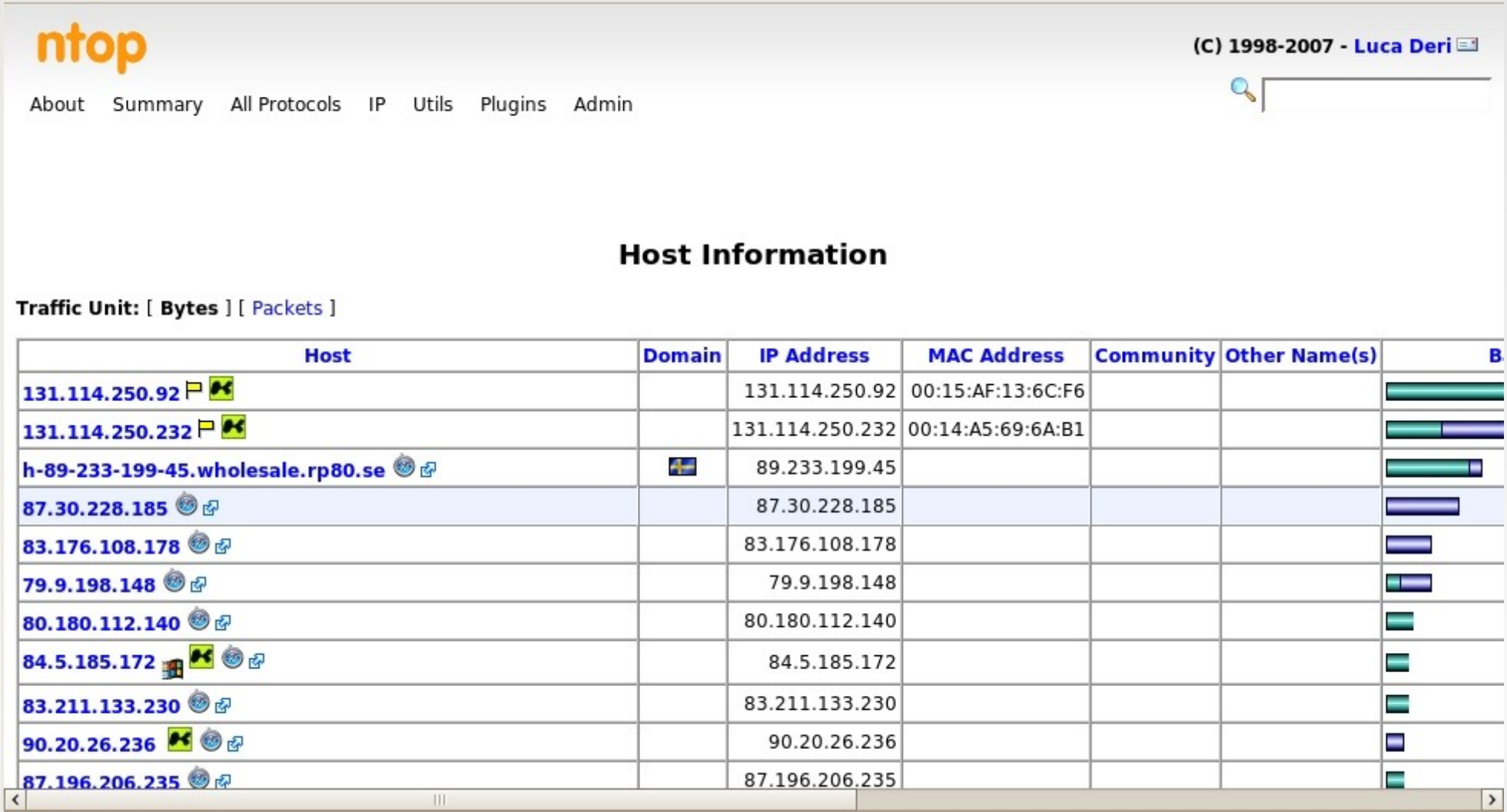
Tutti conoscono il comando top sotto unix : che fornisce in output l'utilizzo delle risorse della singola macchina.

```
top - 12:50:07 up  1:14,  3 users,  load average: 0.48, 0.46, 0.53
Tasks: 104 total,   2 running, 102 sleeping,   0 stopped,   0 zombie
Cpu(s):  2.0%us,  1.0%sy,  0.0%ni, 96.4%id,  0.0%wa,  0.3%hi,  0.3%si,  0.0%st
Mem:    773528k total,   724720k used,    48808k free,    20120k buffers
Swap:  1023736k total,        0k used,  1023736k free,   370600k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 4398 root      15   0  125m  36m  12m S  1.3  4.9   2:44.05 Xorg
 5007 riccardo  15   0  8044 4528 2380 S  0.7  0.6   0:03.03 gconfd-2
 5035 riccardo  15   0 58760  23m  17m S  0.3  3.1   0:21.72 gnome-panel
 7311 riccardo  15   0  2984 1336 1056 R  0.3  0.2   0:00.40 top
 7353 riccardo  15   0 43628  14m  11m S  0.3  2.0   0:00.83 gnome-screensho
    1 root      15   0  3060 1984  660 S  0.0  0.3   0:02.23 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    3 root      RT   0     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    4 root      10  -5     0    0    0 S  0.0  0.0   0:00.81 events/0
    5 root      10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    6 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
   55 root      11  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   57 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
   72 root      16   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
   73 root      15   0     0    0    0 S  0.0  0.0   0:00.02 pdflush
   74 root      11  -5     0    0    0 S  0.0  0.0   0:00.00 kswapd0
   75 root      11  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
```

# ntop

- ntop fornisce in output l'utilizzo della rete



# ntop

## Cosa è e cosa può fare ntop?

- ntop è un tool per l'analisi passiva del traffico di rete multi piattaforma
- Monitoraggio di rete
- Ottimizzazione della rete
- Individuazione problemi di rete

# ntop

## Cosa posso vedere con ntop ?

- Distribuzione del traffico per protocollo (TCP,UDP,ICMP,IPX,NetBIOS, Appletalk)
- Distribuzione del traffico per servizio (broadcast, web, mail, FTP, P2P)
- Distribuzione del traffico per sorgente / destinazione
- Matrici di comunicazione (”chi parla con chi”)
- Connessioni attive per ogni client
- La percentuale di banda occupata
- Traffico Voip (SIP, Cisco SCCP) Monitoring
- Storico delle sessioni tcp

# ntop

## Statistiche del Traffico

| | |
|---|---|
| TRAFFIC DISTRIBUTION | Local (subnet) traffic, local vs. remote (outside specified/local subnet), remote vs. local. |
| PACKETS DISTRIBUTION | Total number of packets sorted by packet size, unicast vs. broadcast vs. multicast and IP vs. non-IP traffic. |
| USED BANDWIDTH | Actual, average and peak bandwidth usage. |
| PROTOCOL UTILIZATION AND DISTRIBUTION | Distribution of the observed traffic according to both protocol and source/destination (local vs. remote). |
| LOCAL SUBNET TRAFFIC MATRIX | Monitored traffic between each pair of hosts in the subnet. |
| NETWORK FLOWS | Traffic statistics for user-defined flows (traffic of particular interest to the user) |

# ntop

## ntop e  problemi di rete

- Rileva indirizzi ip duplicati
- Interfaccie in modalità promiscua
- Client ntp mal configurati, Dns che non usano la cache uso di protocolli superflui
- Identificazione di subnet, router e host configurati come router
- Uso eccessivo della banda

# ntop

## ntop e sicurezza

- La maggior parte degli attacchi in una rete provengono da se stessa, per questa ragione ntop identifica potenziali buchi di sicurezza come IP spoofing, Denial of service,portscan e attacchi synflood
- Quando viene individuata una violazione o una mal configurazione ntop genera un allarme per l'amministratore (via mail, SNMP traps o SMS)  e (dove possibile) blocca l'attacco
- Tutte le informazioni sul traffico sono archiviate in un database, e possono essere utilizzate per capire e prevenire gli attacchi

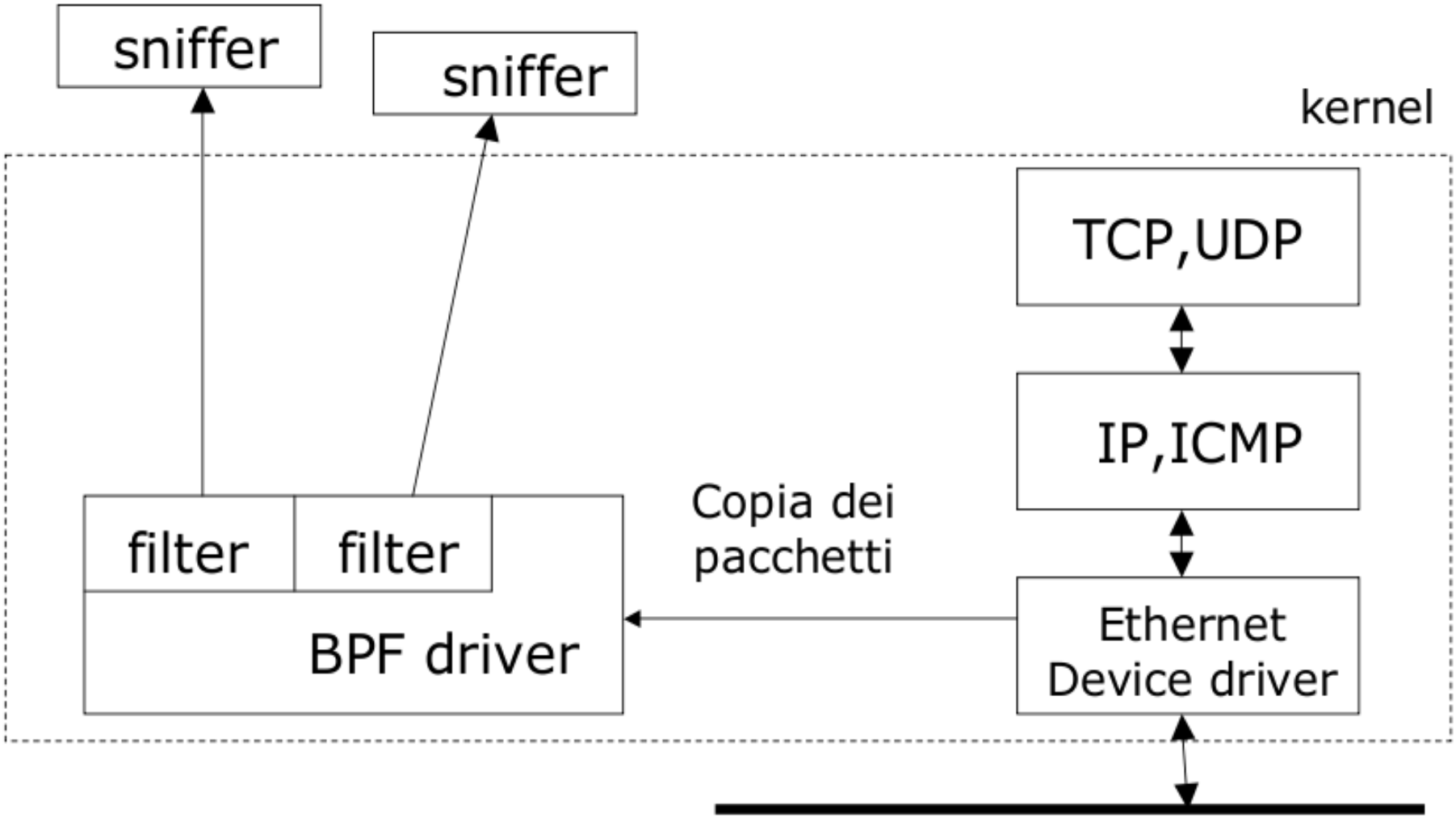
# ntop

## Ntop e NetFlow /Sflow

- ntop supporta NetFlow(v1/5/7/9) e Sflow(v2/5)
- NetFlow è un protocollo proprietario di cisco per collezionare i flussi passanti per i router
- Sflow è uno standard per monitorare reti switchate ad alta velocità basato sul sampling
- I flussi vengono raccolti su interfacce virtuali definite dall'utente si possono definire più interfacce in modo indipendente
- Ntop può monitorare simultaneamente netflow,sflow e pcap

# ntop

## Packet Capture : LibPcap



# ntop

## Linux Packet Capture

- Linux risulta inefficiente in presenza di una grande quantità di traffico di rete.

| Capture Mode | Linux 2.4 [w/o Polling] | Linux 2.6 w/Polling | FreeBSD w/Polling | Windows |
|---|---|---|---|---|
| Libpcap | 0,1% | 0,8% | 74,7% | 28,6% |
| Libpcap mmap() | 1,1% | | | |
| Kernel Module | 1,5% | 9,7% | | |

La tabella illustra la % di pacchetti catturati sul totale inviato.

# ntop

## Linux Packet Capture Problem

- Per monitorare una rete a 100 Mbit è sufficiente un normale pc e tools basati sulle libpcap
- I problemi nascono quando ci troviamo a monitorare reti sopra i 100Mbit perché si ha una grossa percentuale di pacchetti persi
- Linux con il kernel vanilla non è un buon sistema per monitorare la rete

# ntop

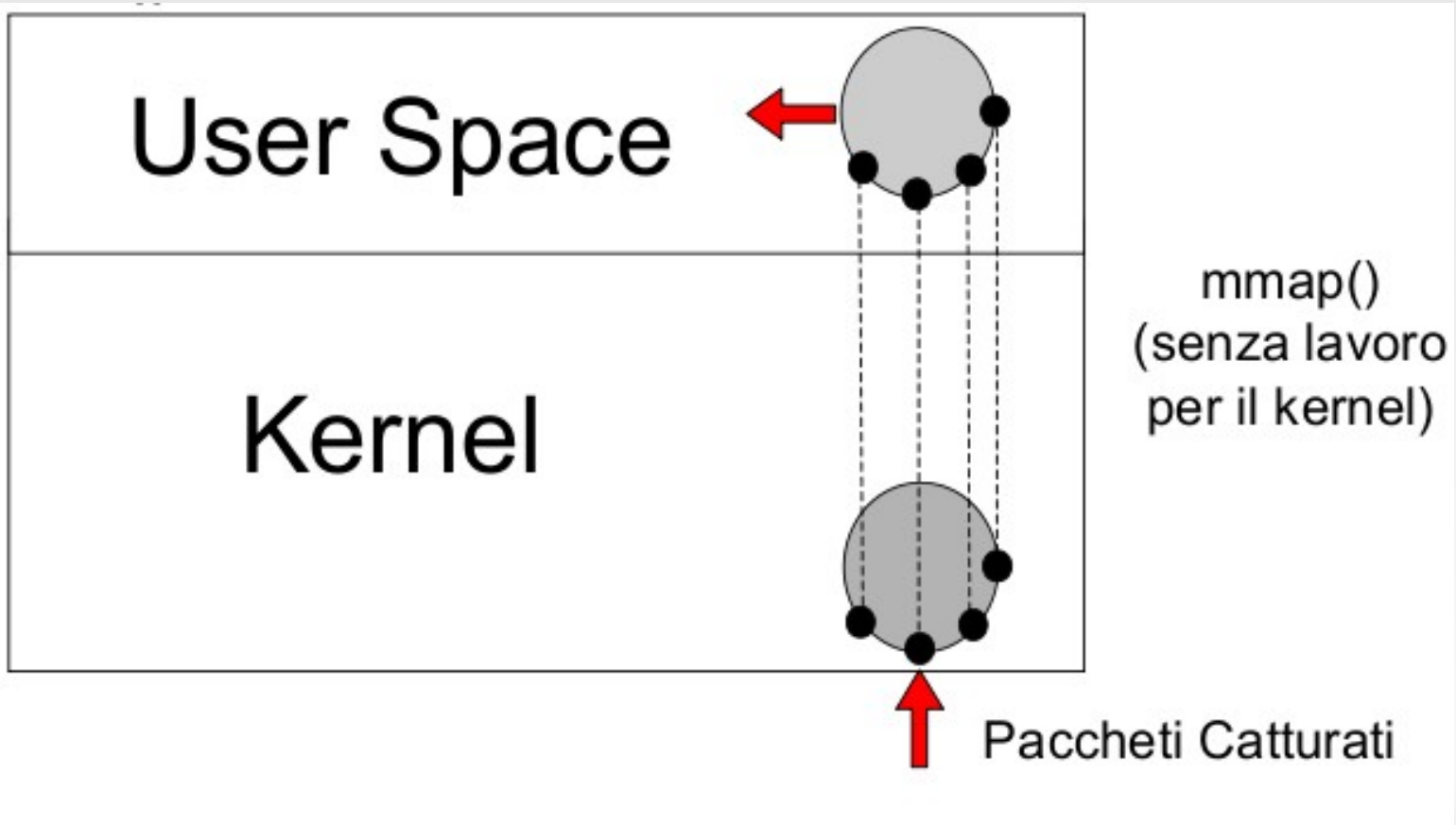
## Monitoraggio con Linux?

- Linux Kernel polling (Linux 2.6.x+NAPI) aiuta ma non abbastanza
- FreeBSD con il device Polling è piu performante di Linux
- Esiste una soluzione che rende linux piu performante?

# ntop

## Soluzione Proposta: PF_RING: Socket Packet Ring

- Attraverso l'uso di buffer circolari riusciamo a incrementare notevolmente la cattura di pacchetti



# ntop

## Statistiche con PF_RING

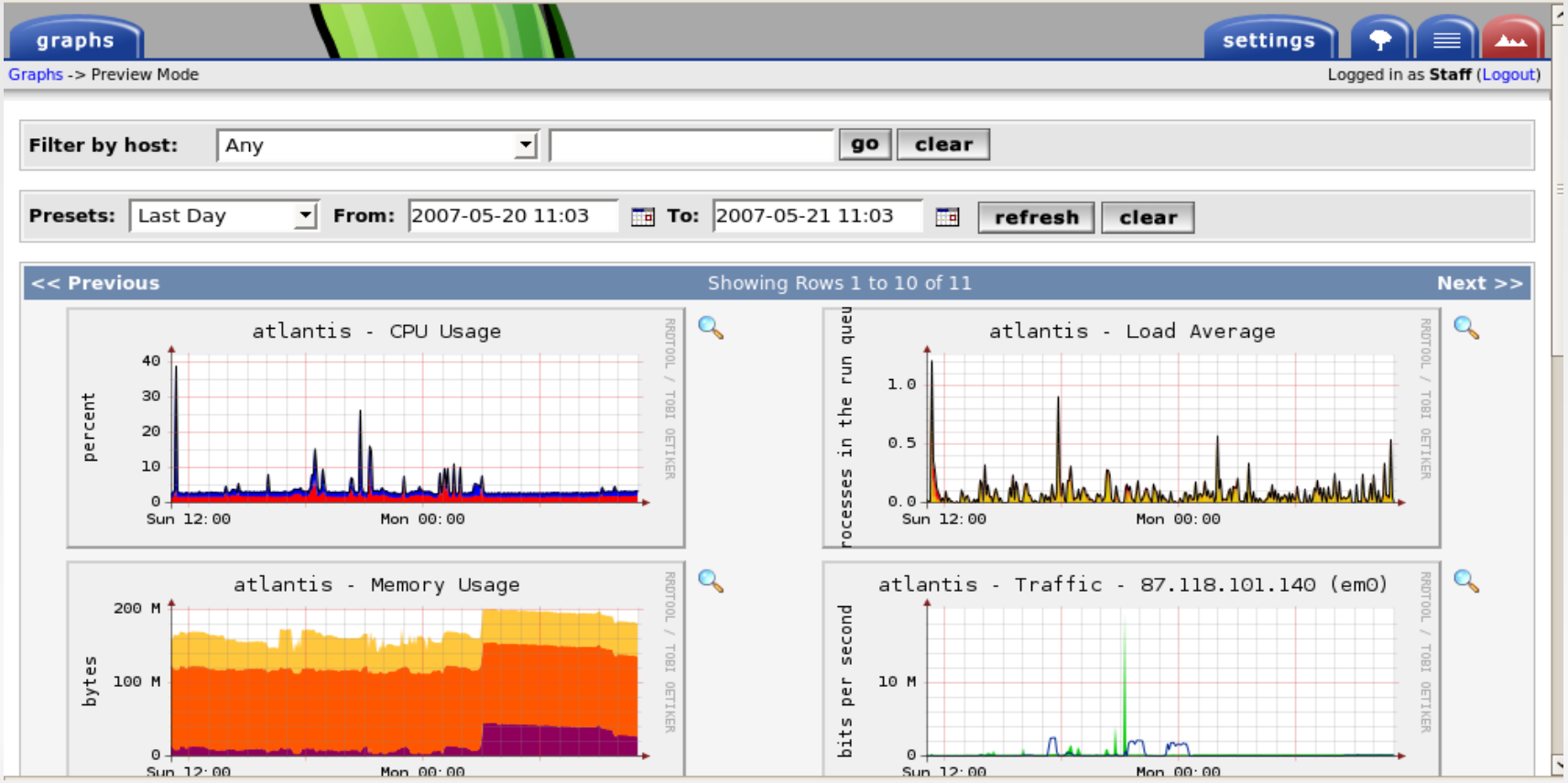
- Linux con PF_RING riesce a superare le performance delle LibPcap e per pacchetti di 1500 byte a superare FreeBSD

| Packet Size (Bytes) | Speed (Mbit) | Speed (Pkt/sec) | Linux 2.6.1 with NAPI and standard libpcap | Linux 2.6.1 with NAPI and Ring | FreeBSD 4.8 with Polling |
|---|---|---|---|---|---|
| 64 | 90 | 175'000 | 2.5% | 75.7% | 97.3% |
| 512 | 710 | 131'000 | 1.1% | 47% | 47.3% |
| 1500 | 836 | 70'000 | 34.3% | 92.9% | 56.1% |

# ntop

## Altri programmi per il monitoraggio

- Cacti: raccoglie via SNMP i parametri in merito a diversi componenti del target e li presenta sotto forma grafica, andamento attuale e andamento totale, ma non una panoramica della rete.



# ntop

## ntop VS cacti

- Cacti è piu indicato nel monitorare risorse precise come host, ha bisogno del database e di una preconfigurazione prima di utilizzarlo
- Ntop è specifico per il monitoraggio di rete non richiede configurazioni prima dell'uso e il database è opzionale se si vuol tenere uno storico del traffico. Ntop supporta protocolli commerciali quindi può essere un'ottima alternativa a software proprietari

# ntop

## Nagios VS Ntop

- Nagios: Il suo scopo è creare una mappa della rete e dei suoi servizi, tenendo sotto controllo la disponibilità degli oggetti monitorati
- La configurazione di nagios è abbastanza lunga perche ha molti file di configurazione, bisogna configurare anche il database e il cgi del proprio web server
- Ntop ha il webserver integrato e non ha bisogno di configurazioni

# ntop

## Conclusioni

- Ntop è un tool per l'analisi passiva del traffico di semplice utilizzo e il suo supporto a protocolli commerciali si offre come valida alternativa a molti software a pagamento
- Il suo punto di forza è la semplicità di installazione semplicità di utilizzo soprattutto grazie all'interfacciaweb
- Altri tool dello stesso autore aumentano le funzioni di ntop
- Nprobe : probe Netflow che colleziona i dati e usa ntop come console centrale, utilizzabile in tutte le reti con router NetFlow enable
- PF_RING : Linux Packet Capture acceleration per kernel vanilla
- nCap wire-speed packet capture per reti da 1 a 10 Gbit