10Gbit/s in več...

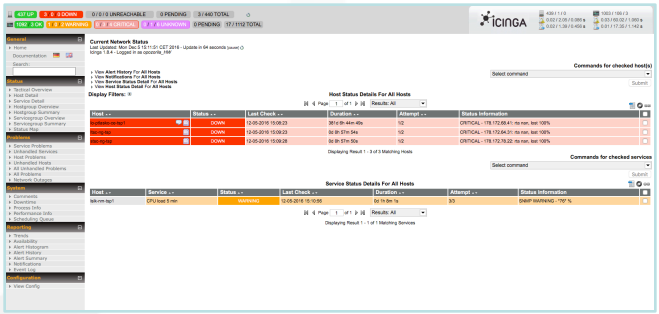
kaj lahko analiziram z običajnim serverjem?

Miha Jemec

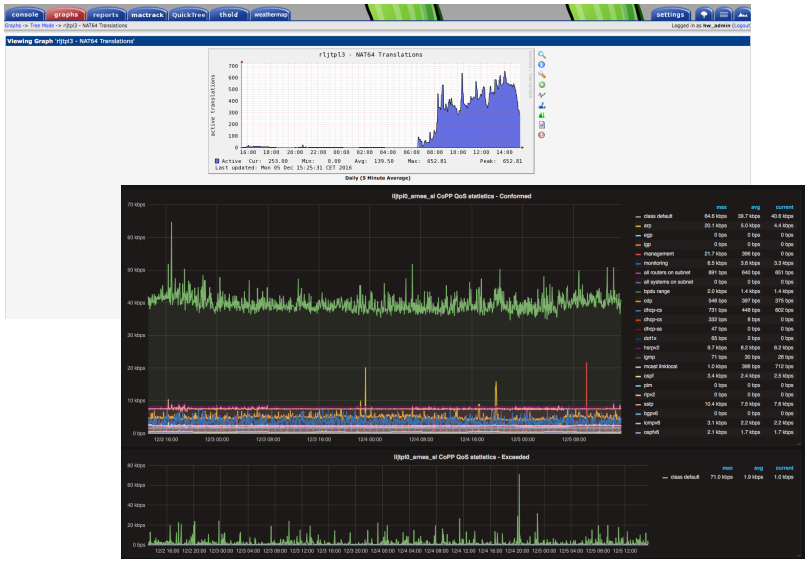
Arnes

miha.jemec@arnes.si

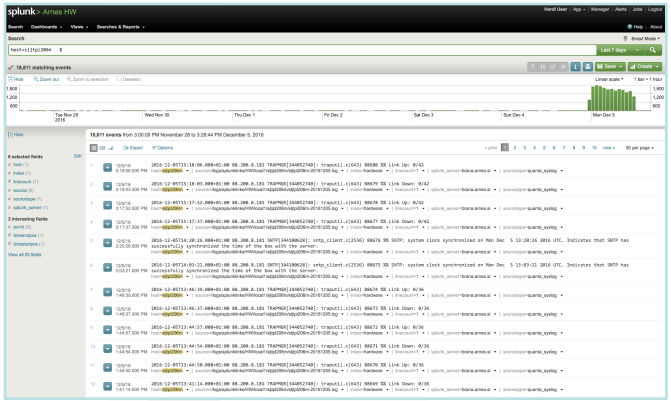
Nadzor



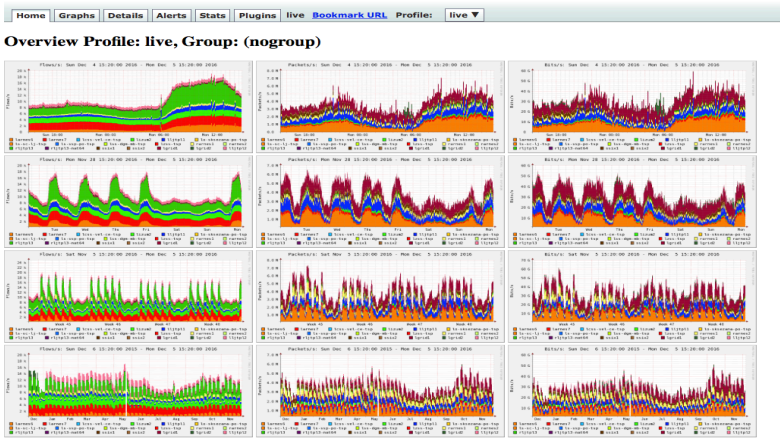
Grafi



Logi



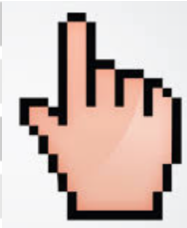
Promet



skripte...

Icinga

lbled1	check output drops	OK	05-12-2016 15:30:27	10d 4h 48m 35s	1/3	OK
lcelje1	check output drops	WARNING	05-12-2016 15:29:26	4d 11h 31m 37s	3/3	Total errors: 4057, Max drop rate: 0.29686% (
ld-ic-lj	check output drops	OK	05-12-2016 15:32:18	0d 0h 1m 44s	1/3	OK
ldomdiplomcev	check output drops	OK	05-12-2016 15:29:05	53d 7h 14m 57s	1/3	OK
ldravog1	check output drops	OK	05-12-2016 15:31:36	10d 4h 47m 26s	1/3	OK
leimv	check output drops	OK	05-12-2016 15:31:27	31d 5h 47m 39s	1/3	OK
lfl-uni-mb	check output drops	OK	05-12-2016 15:29:38	52d 10h 44m 42s	1/3	OK
lfl-uni-mb-kk	check output drops	OK	05-12-2016 15:30:28	60d 9h 8m 39s	1/3	OK
lfov-uni-mb	check output drops	OK	05-12-2016 15:29:36	53d 7h 14m 47s	1/3	OK
lgi	check output drops	OK	05-12-2016 15:31:35	18d 9h 7m 38s	1/3	OK
lhmz-rs	check output drops	WARNING	05-12-2016 15:29:29	10d 2h 21m 37s	3/3	Total errors: 36068, Max drop rate: 0.06969%
licpe1	check output drops	OK	05-12-2016 15:33:46	0d 0h 0m 16s	1/3	OK
lijs	check output drops	OK	05-12-2016 15:29:39	0d 9h 9m 24s	1/3	OK
lijs2	check output drops	OK	05-12-2016 15:29:36	53d 7h 14m 47s	1/3	OK
lir-rs1	check output drops	OK	05-12-2016 15:32:25	10d 4h 46m 38s	1/3	OK
lir-rs2	check output drops	OK	05-12-2016 15:33:26	0d 0h 0m 36s	1/3	OK



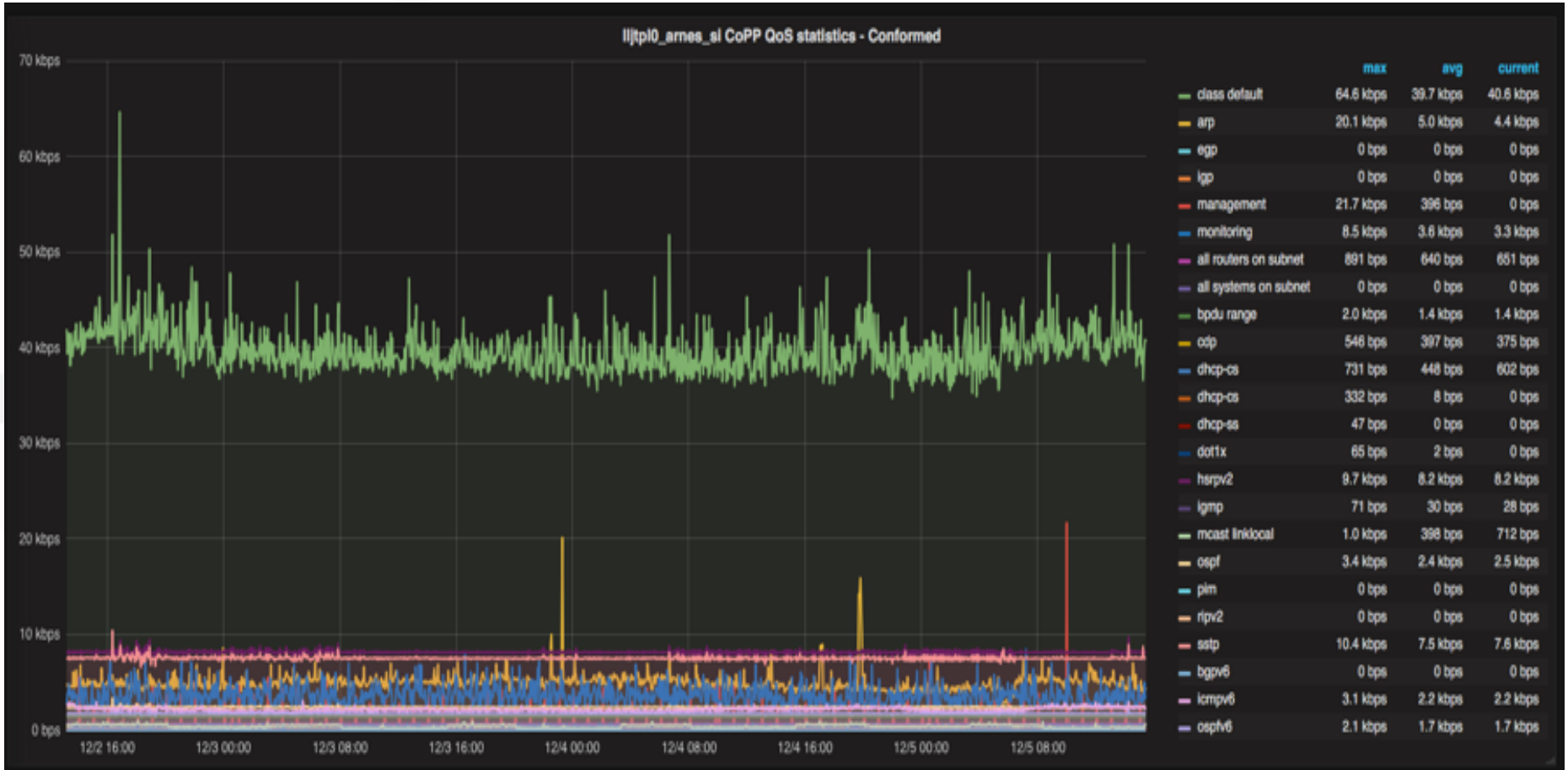
Avg drop rate (%)	Max drop rate (%)
0.00000	0.00000
0.00015	0.06938
0.00000	0.00000

14803541 1481197468 1480948348 Last check time: 08/12/2016 12:44:28 First check time: 05/12/2016 15:32:28 Time elapsed: 2 days 21h 12m 0s Last interval: 0 days 0h 5m 0s

Interface	Speed	Description	Total drops	Last drops	Last int drops/s	Max int drops/s	Out Packets total	Out Packets last int	LastInt pkt/s	MaxInt pkt/s	Avg drop rate (%)	Max drop rate (%)	Warn tot	Crit tot	Ignore Yes/No	Last %	& Max Util %
Fa1	100		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/1	1000		589	0	0.00	1.96	397099052	981514	3272	5530	0.00015	0.06938	1	0	0	3	6
Te1/2	1000		0	0	0.00	0.00	32731237	86616	289	2296	0.00000	0.00000	0	0	0	0	2
Te1/3	1000		0	0	0.00	0.00	161710	176	1	3	0.00000	0.00000	0	0	0	0	0
Te1/4	10000		0	0	0.00	0.00	51424051	224971	750	2795	0.00000	0.00000	0	0	0	0	0
Te1/5	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/6	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/7	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/8	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/9	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/10	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/11	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/12	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/13	10000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Te1/14	1000		0	0	0.00	0.00	5167900	46083	154	971	0.00000	0.00000	0	0	0	0	1
Te1/15	10000		0	0	0.00	0.00	353558077	705693	2352	7427	0.00000	0.00000	0	0	0	0	0
Te1/16	1000		0	0	0.00	0.00	0	0	0	0	0.00000	0.00000	0	0	0	0	0
Total:	-	1	589	0	0.00	1.96	-	-	-	-	0.00015	0.06938	1	0	-		

(legend Total first column value: 0-OK, 1-Warning, 2-Critical)

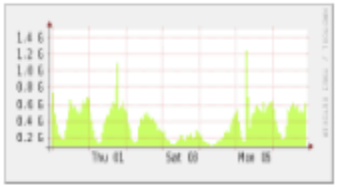
Reset table
Telnet
Back


lljtpl0_arnes_si CoPP QoS statistics - Conformed
70 kbps
60 kbps
50 kbps
40 kbps
30 kbps
20 kbps
10 kbps
0 bps
12/2 16:00
12/3 00:00
12/3 08:00
12/3 16:00
12/4 00:00
12/4 08:00
12/4 16:00
12/5 00:00
12/5 08:00
max avg current
class default 64.6 kbps 39.7 kbps 40.6 kbps
arp 20.1 kbps 5.0 kbps 4.4 kbps
egp 0 bps 0 bps 0 bps
igp 0 bps 0 bps 0 bps
management 21.7 kbps 396 bps 0 bps
monitoring 8.5 kbps 3.6 kbps 3.3 kbps
all routers on subnet 891 bps 640 bps 651 bps
all systems on subnet 0 bps 0 bps 0 bps
bpdu range 2.0 kbps 1.4 kbps 1.4 kbps
cdp 546 bps 397 bps 375 bps
dhcp-cs 731 bps 448 bps 602 bps
dhcp-cs 332 bps 8 bps 0 bps
dhcp-ss 47 bps 0 bps 0 bps
dot1x 65 bps 2 bps 0 bps
hsrpv2 9.7 kbps 8.2 kbps 8.2 kbps
igmp 71 bps 30 bps 28 bps
mcast linklocal 1.0 kbps 398 bps 712 bps
ospf 3.4 kbps 2.4 kbps 2.5 kbps
pim 0 bps 0 bps 0 bps
ripv2 0 bps 0 bps 0 bps
sstp 10.4 kbps 7.5 kbps 7.6 kbps
bgpv6 0 bps 0 bps 0 bps
icmpv6 3.1 kbps 2.2 kbps 2.2 kbps
ospfv6 2.1 kbps 1.7 kbps 1.7 kbps
lljtpl0_arnes_si CoPP QoS statistics - Exceeded
80 kbps
60 kbps
40 kbps
20 kbps
0 bps
12/2 16:00 12/2 20:00 12/3 00:00 12/3 04:00 12/3 08:00 12/3 12:00 12/3 16:00 12/3 20:00 12/4 00:00 12/4 04:00 12/4 08:00 12/4 12:00 12/4 16:00 12/4 20:00 12/5 00:00 12/5 04:00 12/5 08:00 12/5 12:00
max avg current
class default 71.0 kbps 1.9 kbps 1.0 kbps

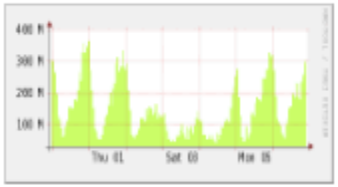
Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

Profile: live

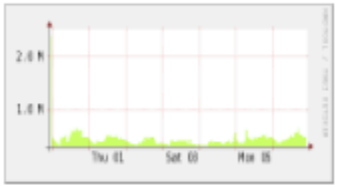
any



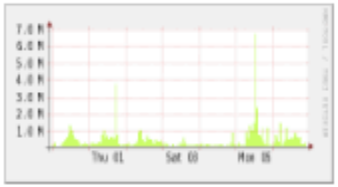
UDP



ICMP

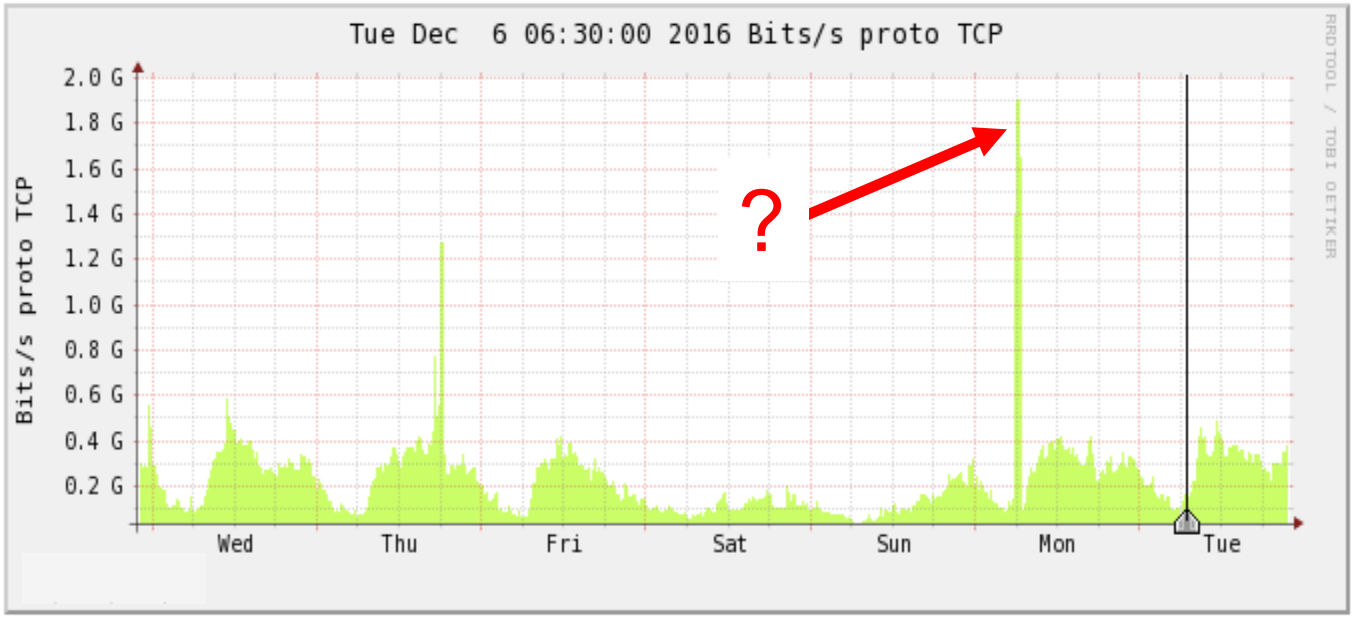


other



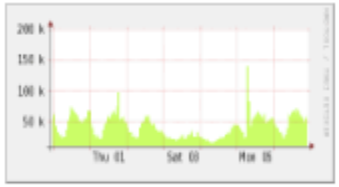
Profileinfo:

Type: live
Max: 800.0 GB
Exp: never
Start: Nov 22 2016 - 21:40 CEST
End: Dec 07 2016 - 08:45 CEST

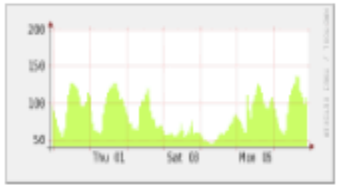


t_{start} 2016-12-06-06-30
t_{end} 2016-12-06-06-30

Packets



Flows



Nekje so težave

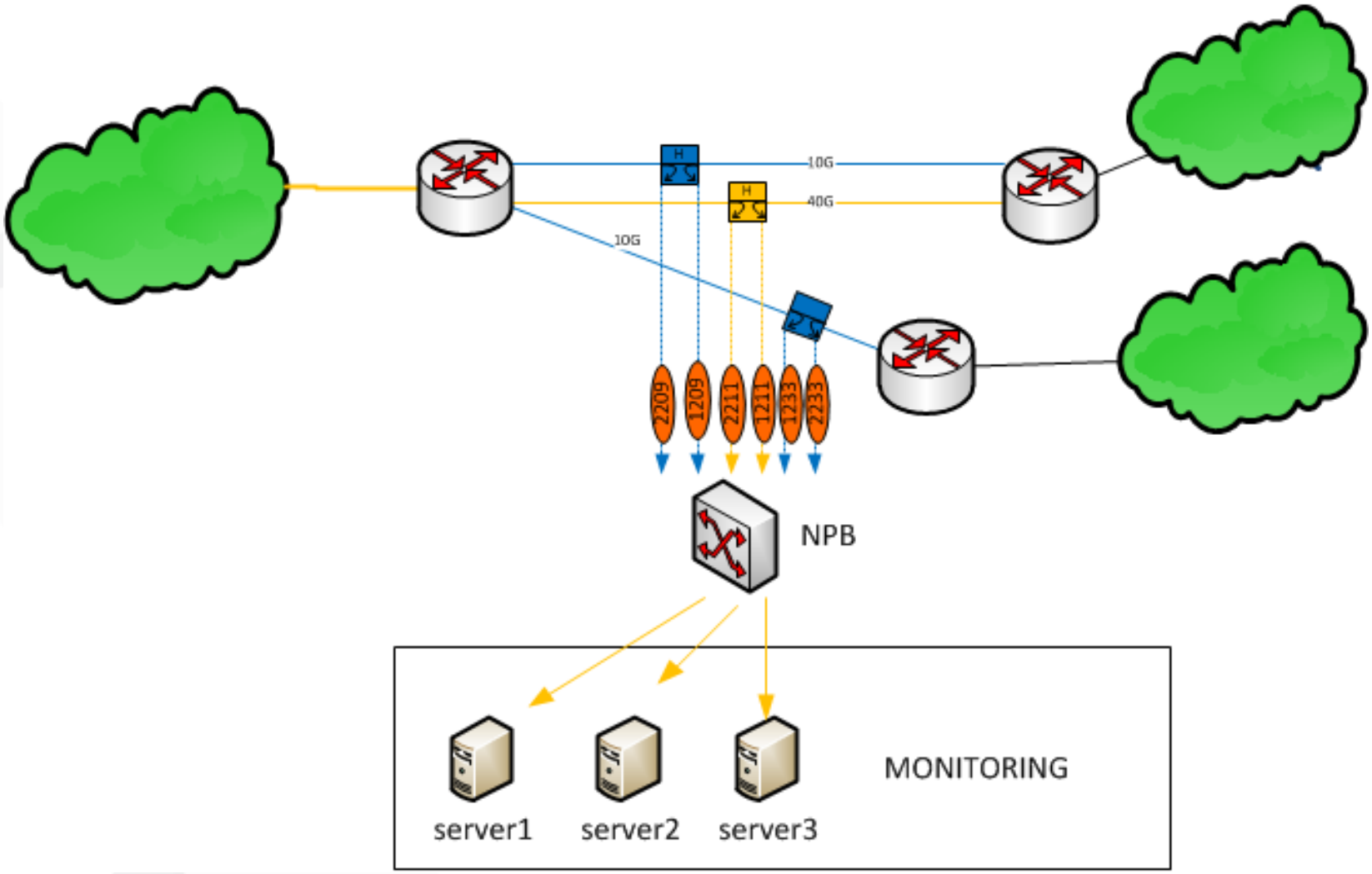
- želiš analizo točno določenega flowa?
- sumiš na DoS? iščeš Top Talkerje?
- ni Netflowa ali je CPU na 100%

Boljša preventiva

- želiš poganjati Snort/Suricato/Bro?
- želiš stvari čimbolj avtomatizirati

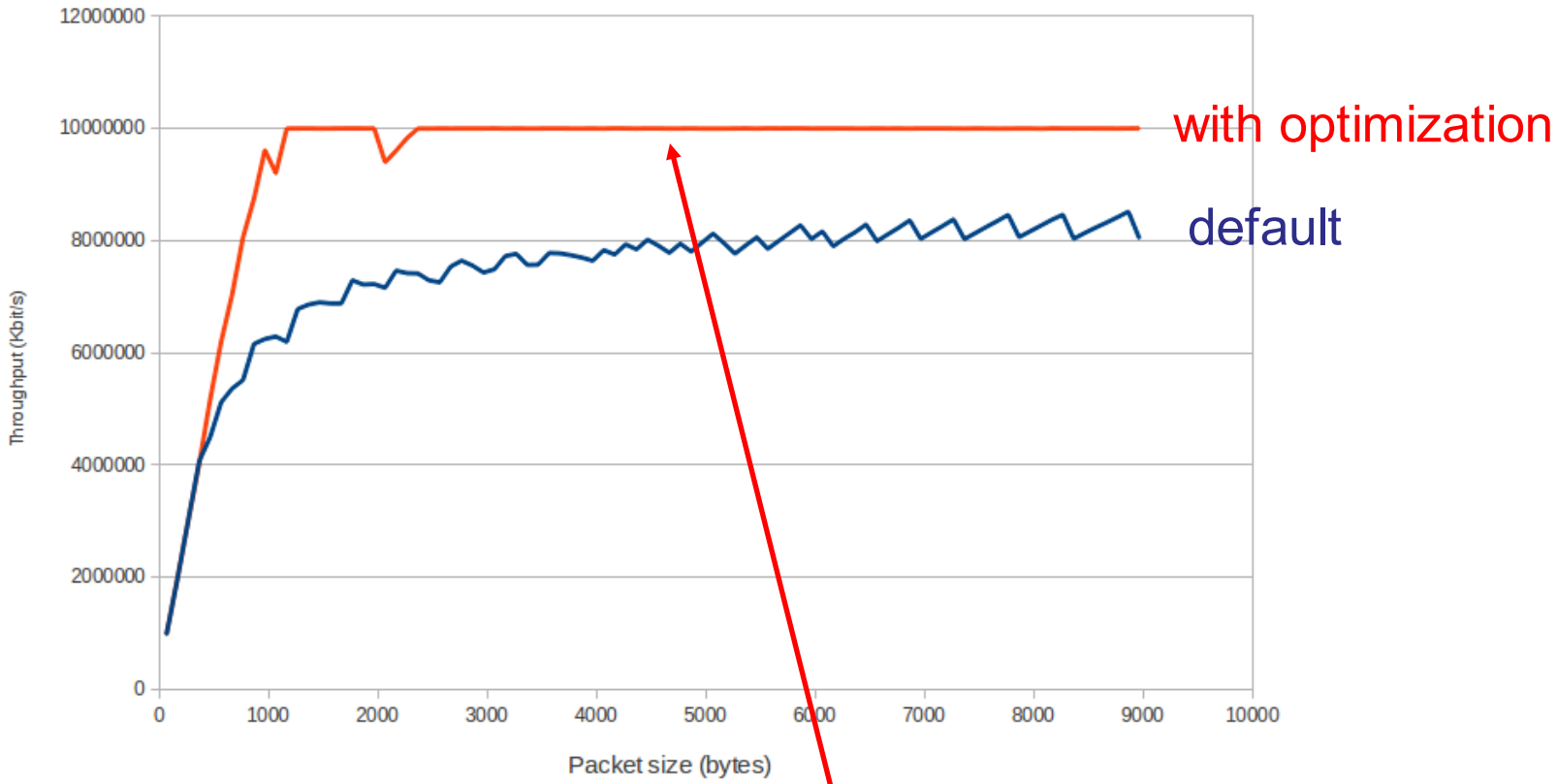
Mirror prometa & analiza

- HW del:
  - optični delilniki
  - NPB stikala
- SW del:
  - običajni serverji
  - opensource programska oprema


10G
40G
10G
2209
1209
2211
1211
1233
2233
NPB
server1
server2
server3
MONITORING

optični spliterji in NPB stikala

- + fiksno okolje
- + promet je vedno in takoj na voljo
- + ni izgubljenih paketov
- + ni del omrežja ”v težavah”
- - velika količina prometa

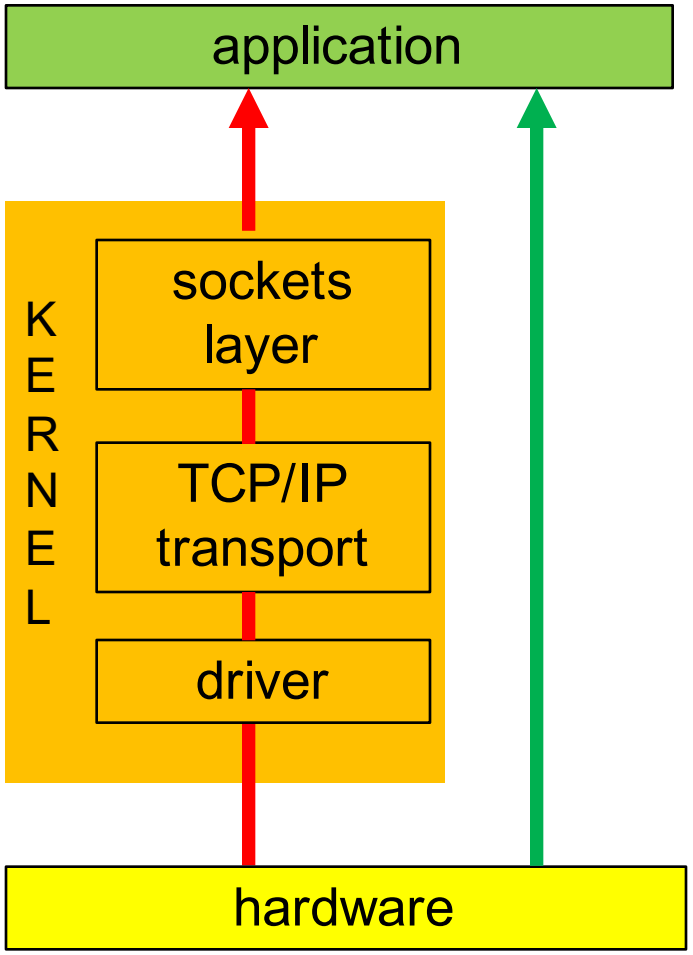


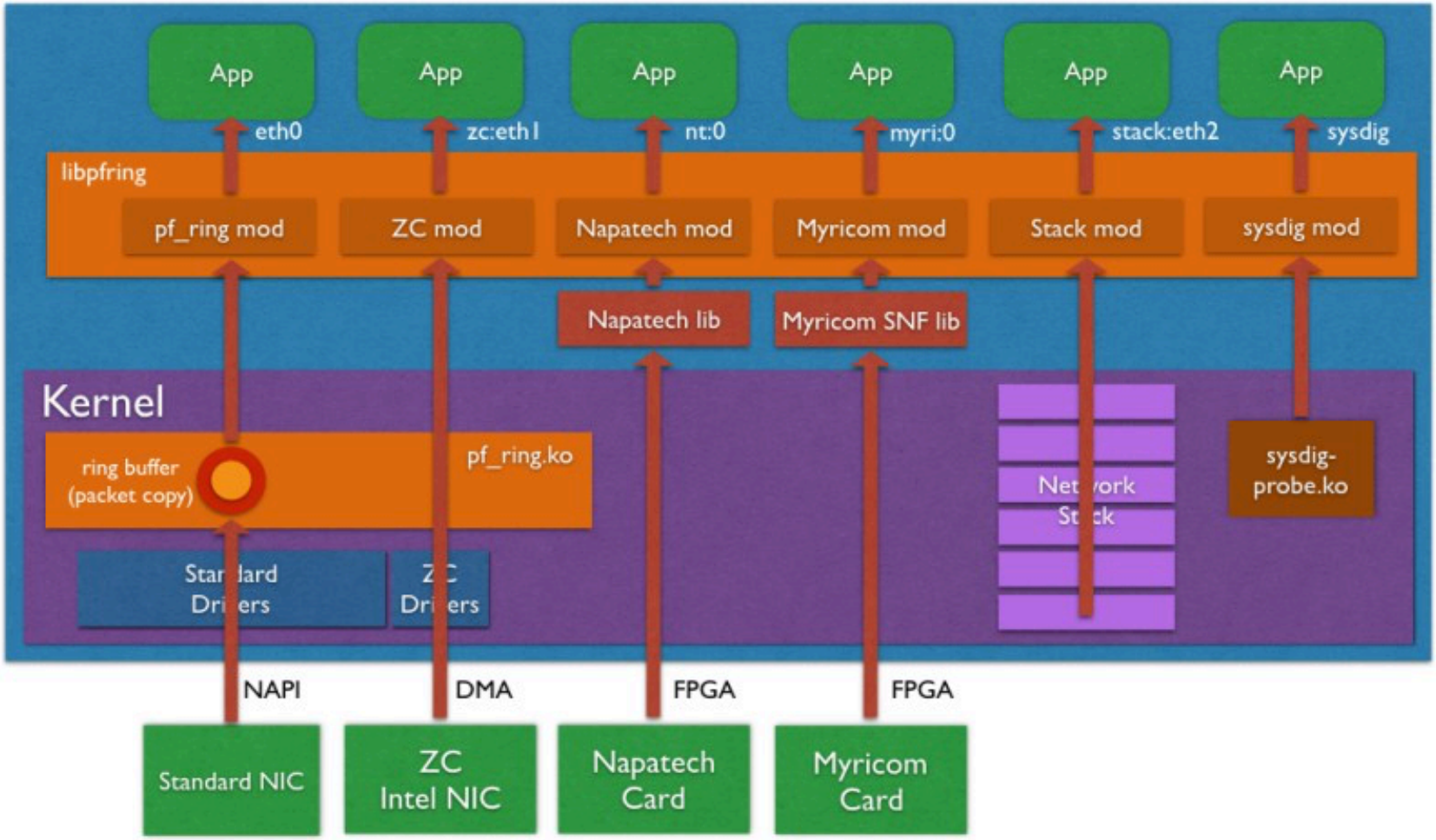
Vanilla Linux - typically up to 1 Mpps

```
cd /proc/sys/net/core
echo "50000" > optmem_max
echo "10000" > netdev_max_backlog
echo "1000000" > wmem_default
echo "1000000" > wmem_max
echo "1000000" > rmem_default
echo "1000000" > rmem_max
```

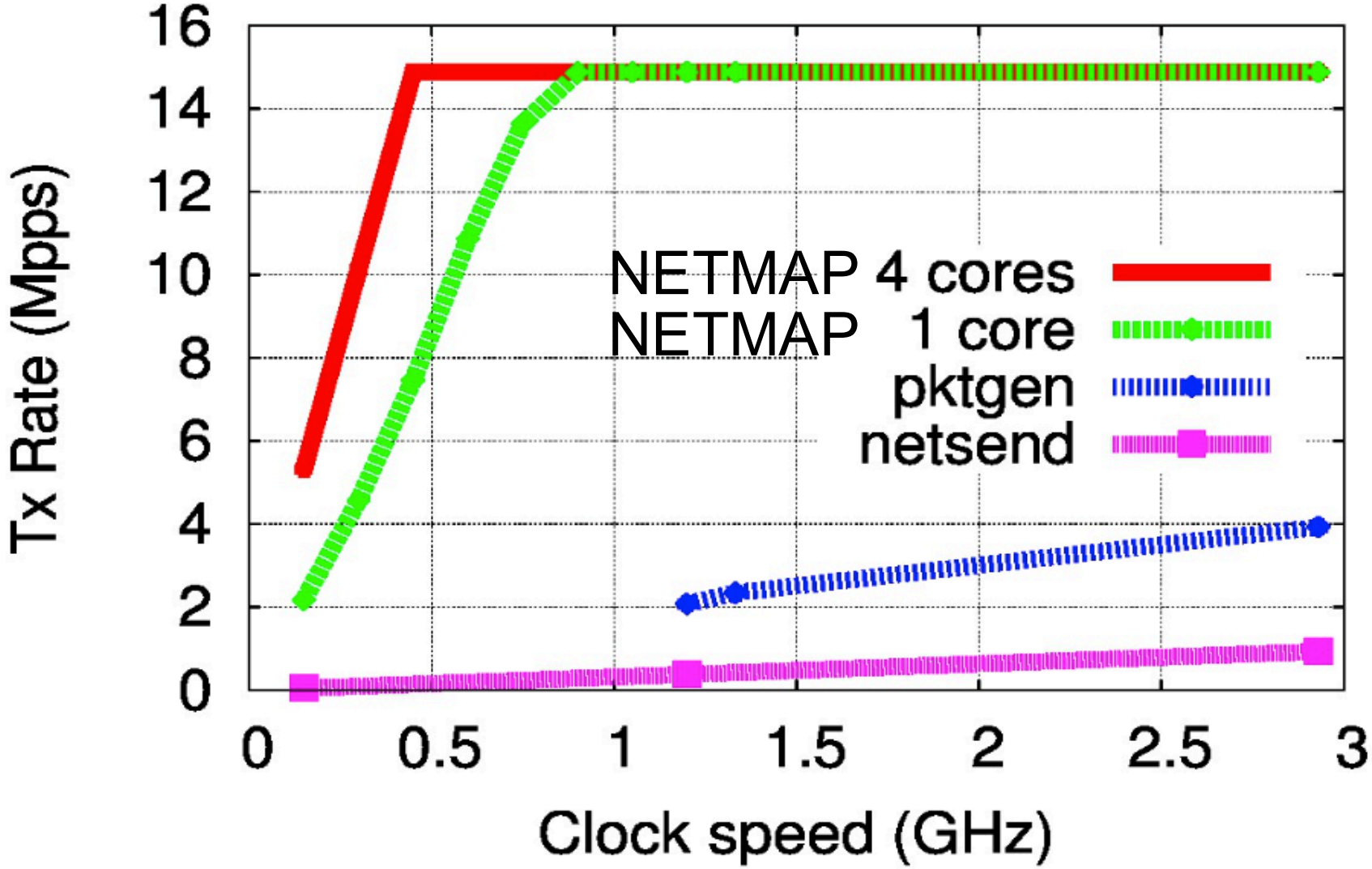
Kernel bypass tehnike

- netmap
- pf_ring zc
- snabswitch
- dpdk




App
App
App
App
App
App
eth0
zc:eth1
nt:0
myri:0
stack:eth2
sysdig
libpfring
pf_ring mod
ZC mod
Napatech mod
Myricom mod
Stack mod
sysdig mod
Napatech lib
Myricom SNF lib
Kernel
ring buffer
(packet copy)
pf_ring.ko
Network
Stack
sysdig-
probe.ko
Standard
Drivers
ZC
Drivers
NAPI
DMA
FPGA
FPGA
Standard NIC
ZC
Intel NIC
Napatech
Card
Myricom
Card

NETMAP performance



vir:netmap.org

Primeri uporabe:

- fastnetmon
- ntopng/nprobe/n2disk/nDPI
- tcpdump/wireshark at 10G/40G/100G
- IDS sistemi

Fastnetmon:

- zelo hiter DoS/DDoS analizator
- DPI analiza paketov za določitev tipa napada
- izvor: netflow/sflow/netmap/pfring/pcap
- akcija: alarm, mail, ExaBGP/BGP flowspec
- Graphite/InfluxDB, Reddis, Mongo
- čas detekcije 1-2 sec, zmogljivost do 12 Mpps
- Linux, opensource

```
FastNetMon v1.0 FastVPS Eesti OU (c) VPS and dedicated: http://FastVPS.host
IPs ordered by: packets (use keys 'b'/'p'/'f' for change) and use 'q' for quit
Threshold is: 35000 pps and 1000 mbps total hosts: 13568

Incoming traffic        171015 pps    384 mbps  11973 flows
159.11.22.33              3309 pps   33.3 mbps     77 flows
159.11.22.33              3116 pps   34.8 mbps      2 flows
159.11.22.33              2567 pps   29.5 mbps      2 flows
159.11.22.33              2439 pps    1.8 mbps     76 flows
159.11.22.33              2364 pps    1.4 mbps     55 flows
159.11.22.33              2104 pps    1.5 mbps     19 flows
159.11.22.33              1938 pps    1.3 mbps     36 flows

Outgoing traffic        225121 pps   1905 mbps  17893 flows
159.11.22.33              3699 pps   39.9 mbps     83 flows
159.11.22.33              3557 pps   37.3 mbps    124 flows
159.11.22.33              2965 pps   32.8 mbps     98 flows
159.11.22.33              2645 pps   29.7 mbps     38 flows
159.11.22.33              2522 pps   26.1 mbps     65 flows
159.11.22.33              2474 pps   26.8 mbps     61 flows
159.11.22.33              2285 pps   18.9 mbps    194 flows

Internal traffic             0 pps      0 mbps

Other traffic               56 pps      0 mbps

Traffic calculated in:  0 sec 14670 microseconds
Packets received:       2308537
Packets dropped:        0
Packets dropped:        0.0 %
```

ntop/nprobe

Open source & license:

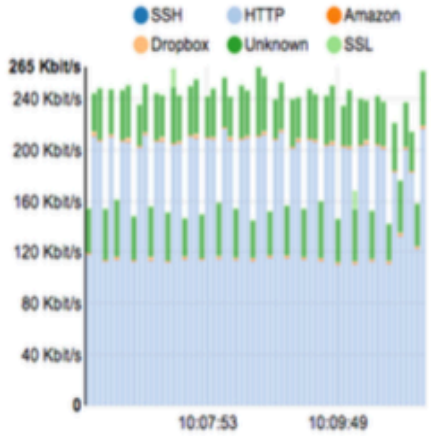
- ntopng: Web based monitoring app
- nDPI: DPI toolkit
- nProbe: 10G Netflow/IPFIX probe
- n2disk/disk2n: packet capture/replay

ntop

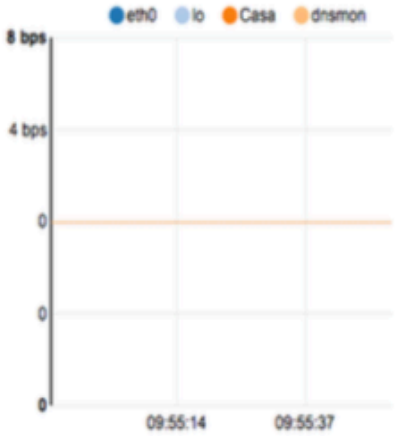
Flows | Hosts | Devices | Interfaces | Search Host

eth0: Top Local Talkers	Actual Traffic
pc-deri.nic.it	243.17 Kbit ↓
dnsmon.nic.it	36.51 Kbit ↑
ninja.nic.it	812.48 bps ↑
pc-leo.nic.it	443.02 bps ↑
pc-sideri.nic.it	439.82 bps ↑
pc-ravazzolo.nic.it	436.63 bps ↑
192.168.17.12	406.24 bps ↑
nsresolv1.nic.it	278.29 bps ↑

eth0: Realtime Top Application Traffic



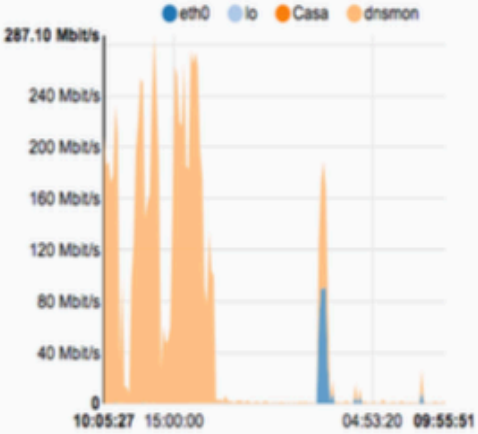
Network Interfaces: Realtime Traffic



eth0: Top Remote Destinations	Actual Traffic
host207-203-dynamic.239-95-r.retail.telecomitalia.it	206.38 Kbit ↓

eth0: Top Application Traffic Last Day View

Network Interfaces: Last Day View



ntopng Enterprise v.2.5.161002
User admin Interface eth0

284.05 Kbps [76 pps]

206.34 Kbps
30.58 Kbps

Uptime: 16 h, 6 min, 45 sec
19,094 Alerts | 71 Hosts | 1,248 Devices | 107 Flows

vir:ntop.org

demo...

- pfring performance
- 10/40G Wireshark
- fastnetmon dos attack detection

Dodatno branje:

- fastnetdata.es.net
  - network troubleshooting
  - linux tuning, tcp tuning

- RedHat - 100Gbit/s challenge