Passive monitoring applicato alle sicurezze

GARR WS5, Roma 26/11/2003

Christian Cinetto

Gruppo Passive Monitoring

- *Christian Cinetto*
- *Michele Sciuto*
- GARR NOC (Network Operation Center)

AGENDA

- Obiettivi
- Passive monitoring
- NetFlow
- Architettura su rete GARR
- Demo
- Applicazioni

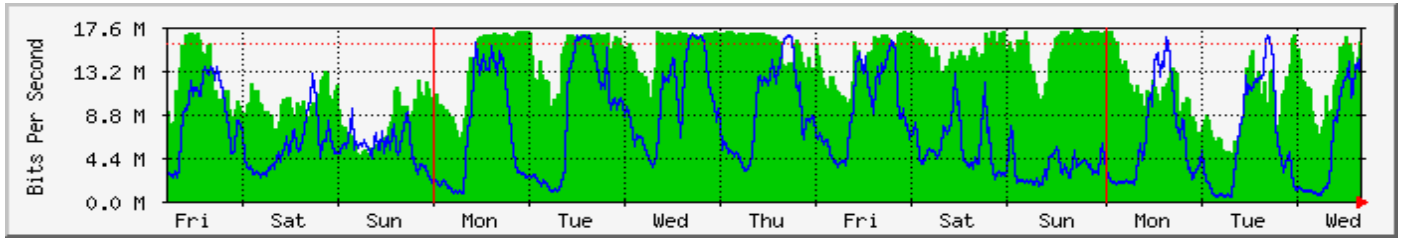
Obiettivi

- Tracciare i DoS fino alla loro sorgente(i)
- Identificare gli hosts compromessi
- Identificare gli hosts che occupano piu' banda
- Distinguere il tipo di traffico (smtp, web, p2p, etc.)
- Tracciare le direttrici del proprio traffico
- Analisi per aggregati (routers o sottoreti)

```
CPU utilization for five seconds:
99%/98%; one minute: 99%; five minutes: 99%
```

! ! !

? ? ? ? ? ?



Strumenti disponibili

Per interventi di sicurezza proattivi… o quasi

- utilizzo ACL : non ottimale (non sempre risolutive, CPU alle stelle)
- packet sniffing : laborioso, non scalabile
- Altri : disponibilità di risorse limitata

Abbiamo uno storico del "cosa oltre che del quanto" passa nella rete?

E se andassimo oltre MRTG?

Trade-off : costo dell'investimento(disco,cpu,RAM,human)

Vs.

livello di dettaglio e real time desiderato

MONITORING

Differenti approcci per scopi differenti

Passive	Active
• Sniffer; schede dedicate (OCxMon) • Built-in devices per snmp, **NetFlow** …	• Iniezione di custom-traffic nella rete • Apparati di sincronizzazione (Es. GPS)

Adatto a …

Analisi e accounting del traffico di produzione	Analisi di performance di rete, QoS

NetFlow

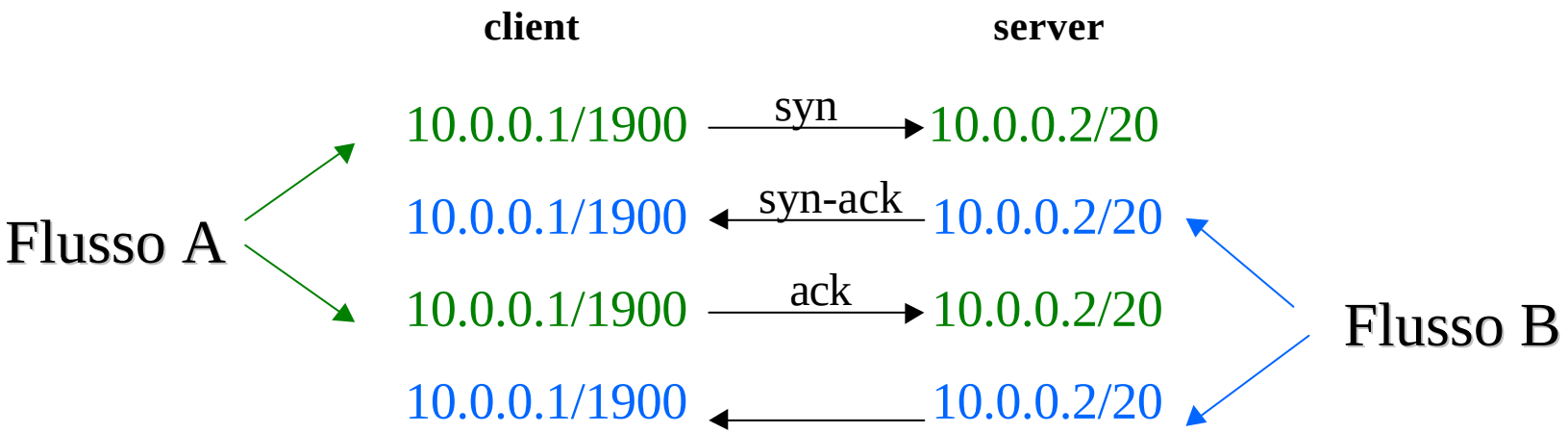
- Feature IOS CISCO dalla 11.* (1996)
- Standard de facto, implementato anche da
  Juniper®, Enterasys®, Extreme®, Foundry®, Riverstone®
- Memorizza i “flussi” in una cache e permette
  l’export dei dati verso un “collector-box”
- Diversi software che permettono l’analisi
  (sia open-source che commerciali)
  - Scalabilità: testato fino a 10G

Flow-based Passive Monitoring

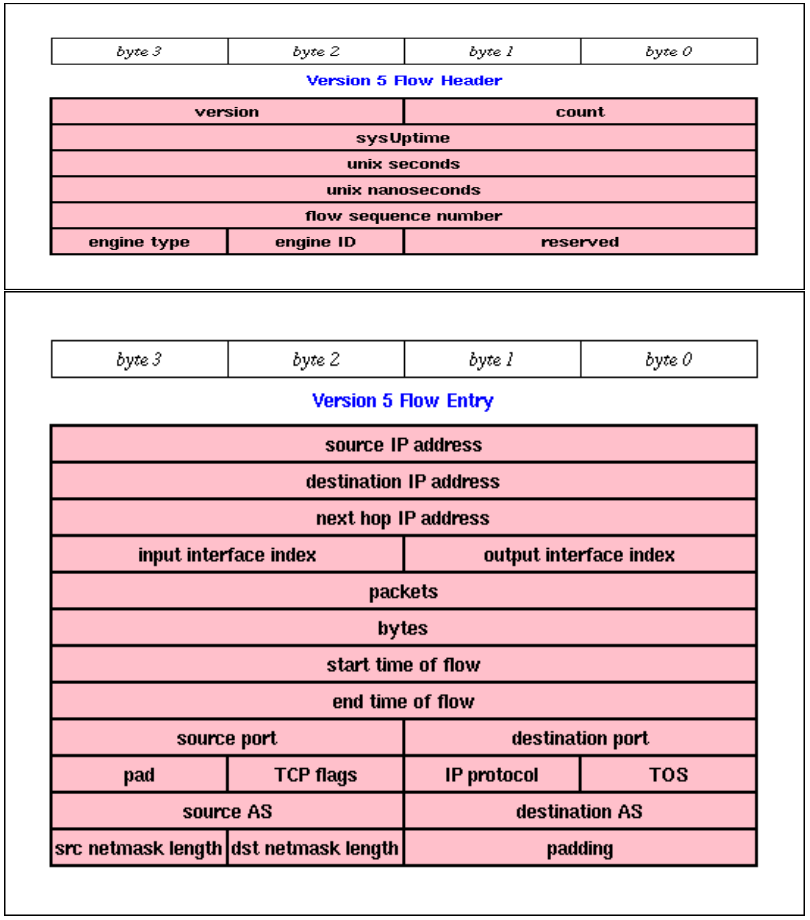
Un flusso NetFlow è definito come una :

" serie unidirezionale di pacchetti IP che viaggiano da una coppia IP/Porta sorgente ad una destinazione, entro un certo intervallo di tempo, avendo definito un protocollo di livello 3 ed un TOS"

ES: UNICA SESSIONE TCP!!!



NetFlow PDU V5



Version 5 Flow Header

byte 3	byte 2	byte 1	byte 0
version		count	
sysUptime			
unix seconds			
unix nanoseconds			
flow sequence number			
engine type	engine ID	reserved	

Version 5 Flow Entry

byte 3	byte 2	byte 1	byte 0
source IP address			
destination IP address			
next hop IP address			
input interface index		output interface index	
packets			
bytes			
start time of flow			
end time of flow			
source port		destination port	
pad	TCP flags	IP protocol	TOS
source AS		destination AS	
src netmask length	dst netmask length	padding	

Collector-Tools

flow-tools

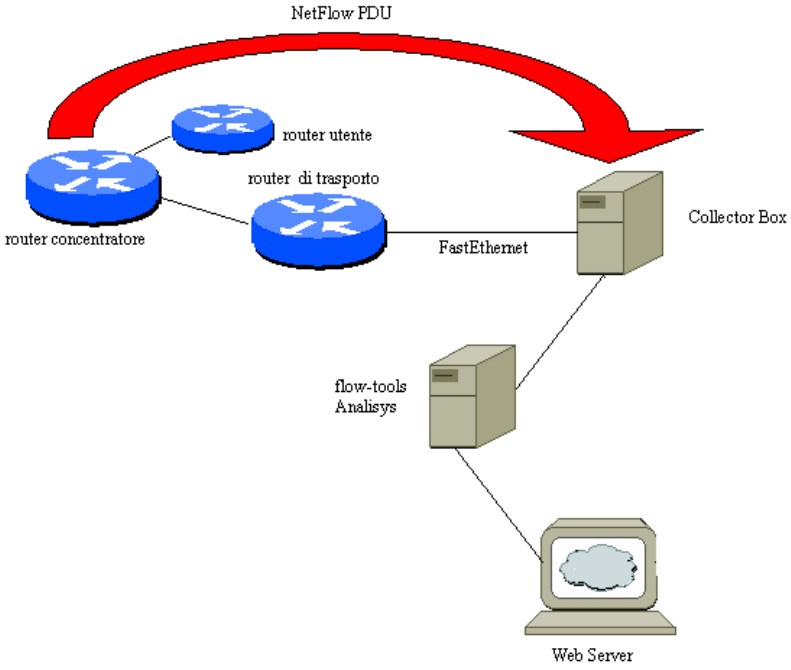
Insieme di tools realizzati alla Ohio State University (OSU) dal 1996

Principali caratteristiche:

- Collezione dati
- Duplicazione verso altri collector
- Concatenazione di report (ad es. nel tempo)
- Filtraggio di ciascun campo NetFlow
- Matrice di report
- Visualizzazione immediata
- Mailing-list attiva e aggiornamento costante

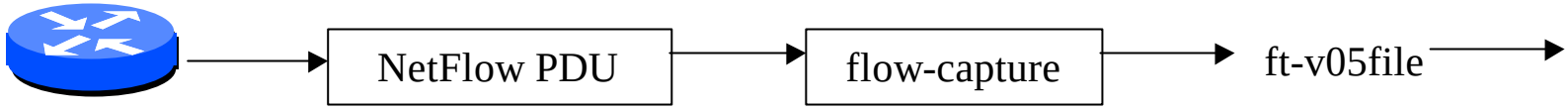
Implementazione GARR

NetFlow e' stato implementato sulla rete GARR negli ultimi 2 anni secondo il seguente schema di principio

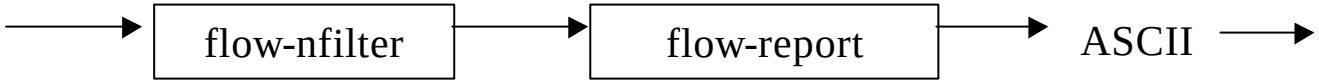


Architettura GARR (dettaglio)

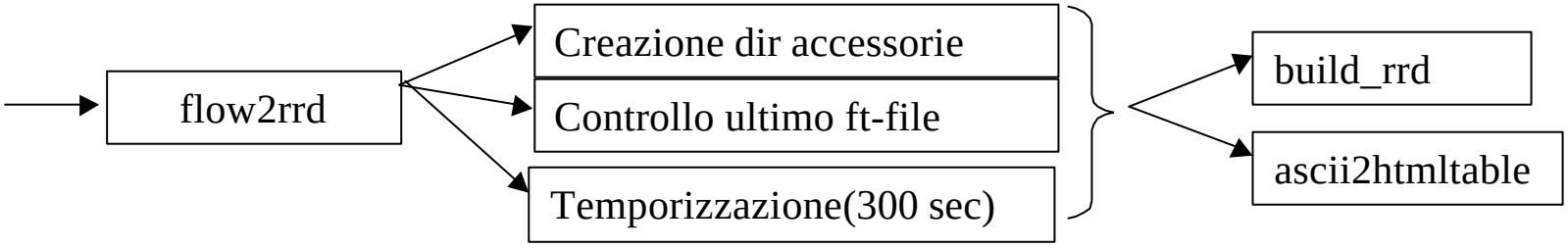
Acquisizione ed archiviazione: router->raw (flow-tool style)



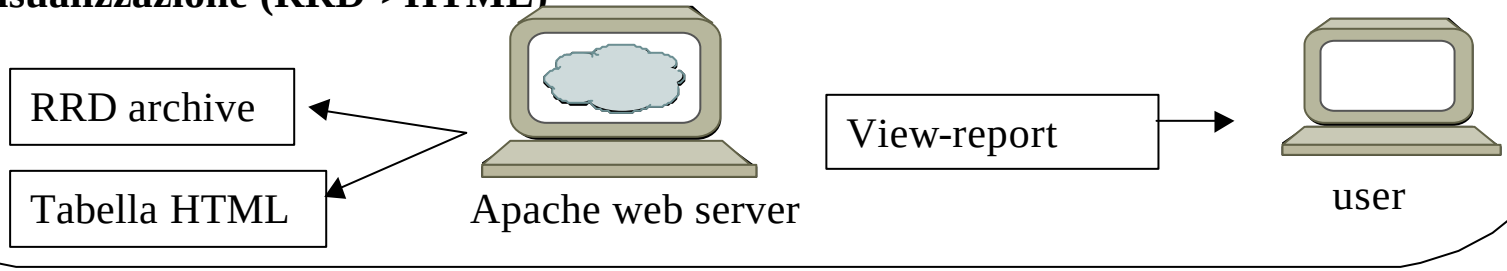
Elaborazione: raw→ASCII



Creazione RRD (ASCII->RRD)

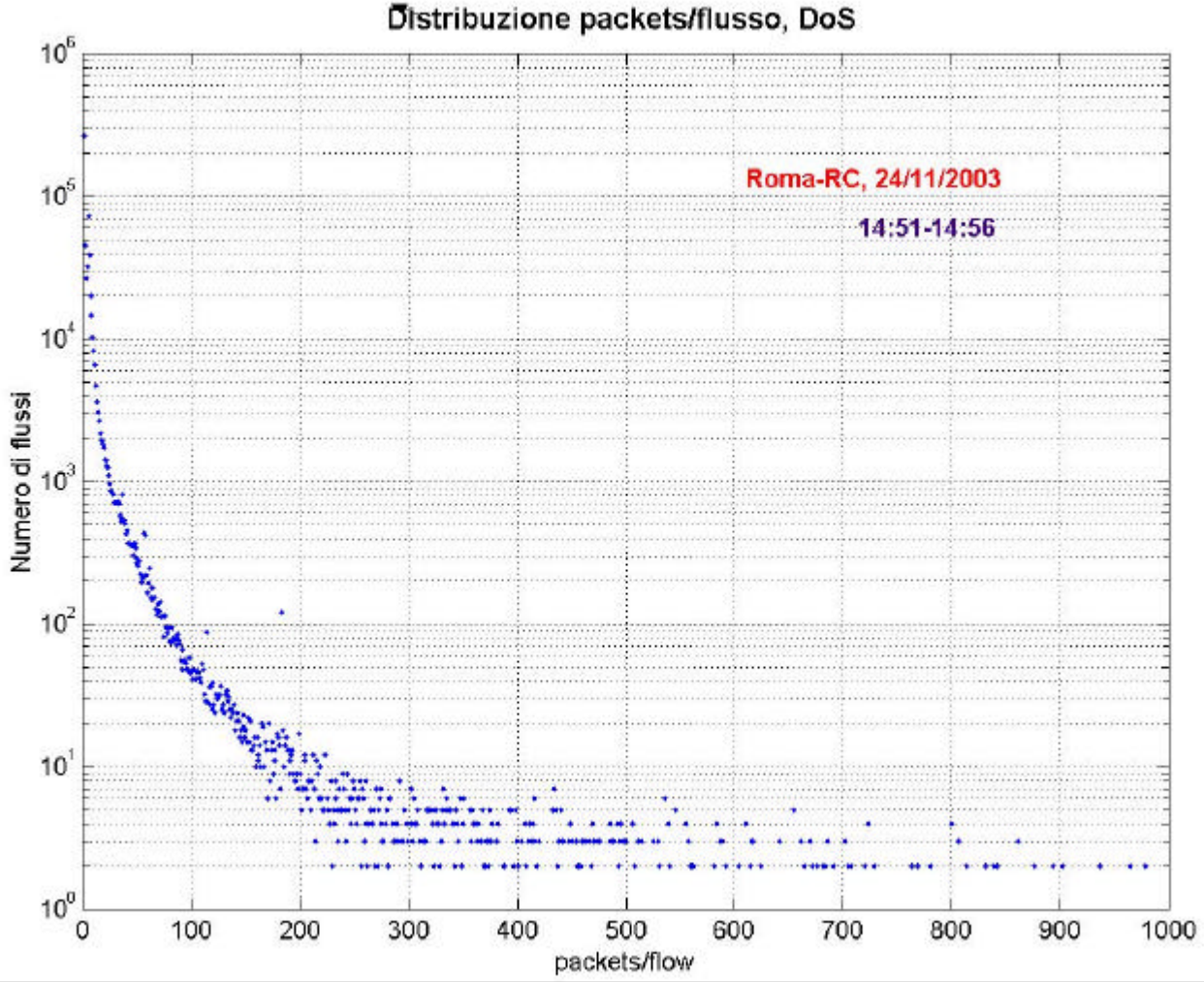


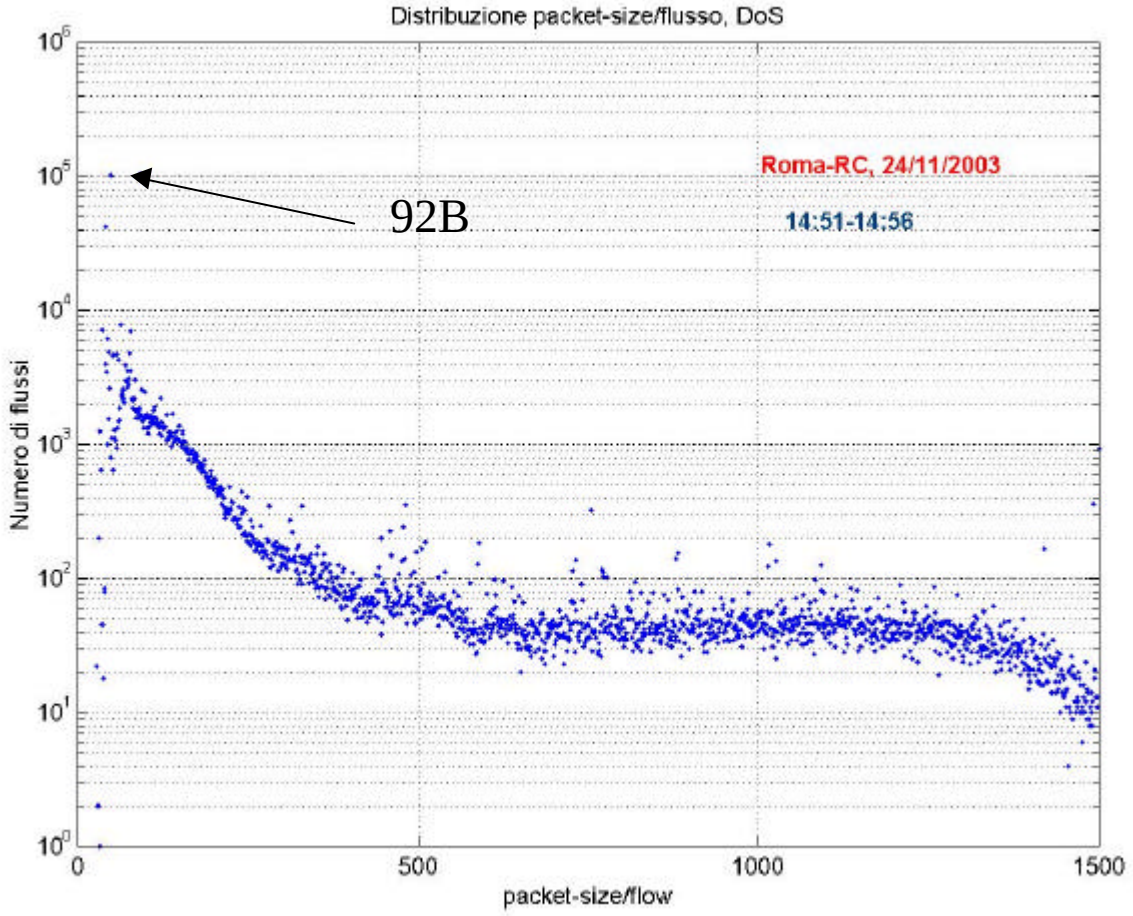
Visualizzazione (RRD->HTML)

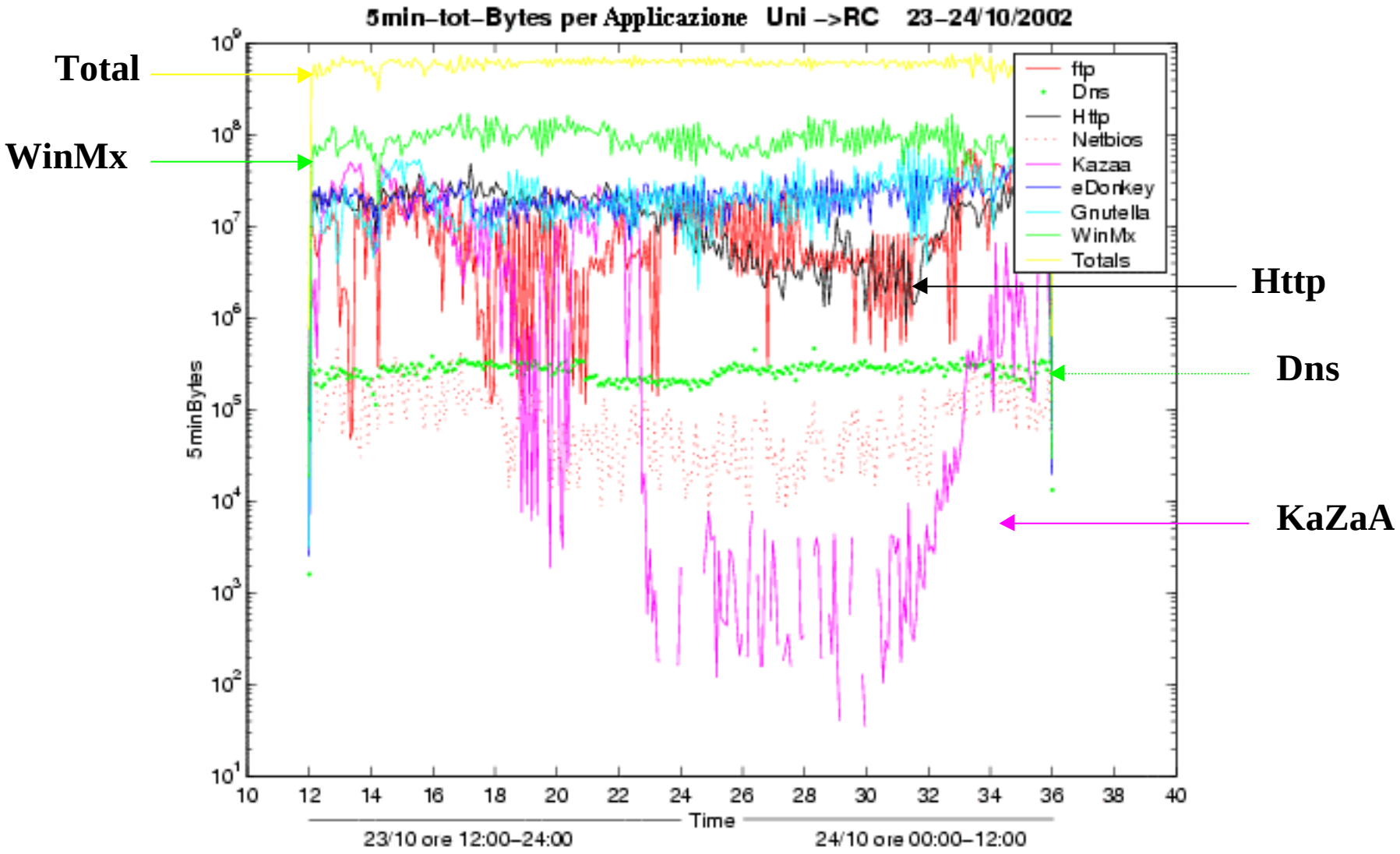


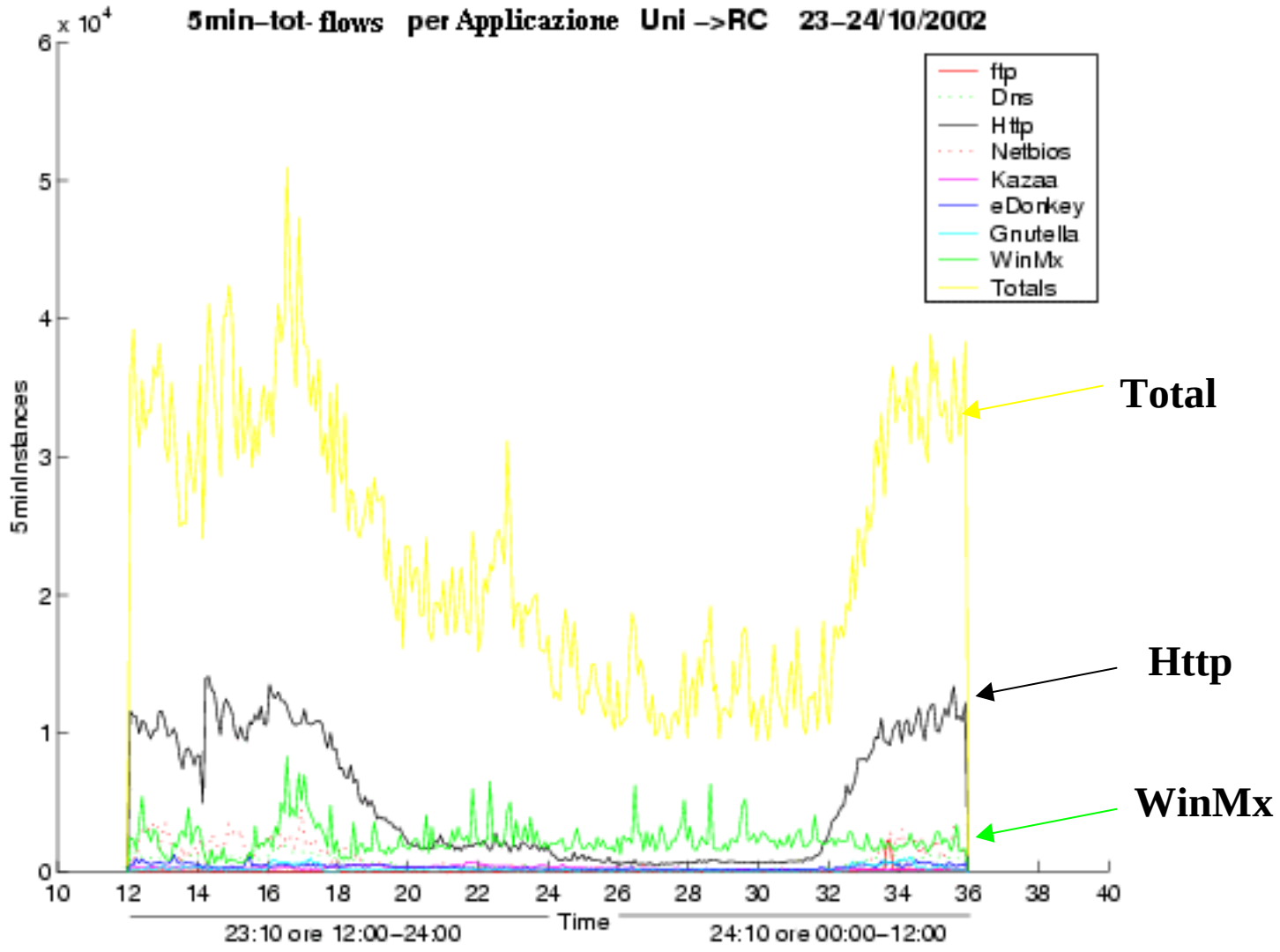
GARR-NetFlow report

DEMO


Distribuzione packets/flusso, DoS
Roma-RC, 24/11/2003
14:51-14:56
Numero di flussi
packets/flow
10^0
10^1
10^2
10^3
10^4
10^5
10^6
0
100
200
300
400
500
600
700
800
900
1000


Distribuzione packet-size/flusso, DoS
Roma-RC, 24/11/2003
14:51-14:56
92B
Numero di flussi
packet-size/flow
0
500
1000
1500


5min–tot–Bytes per Applicazione Uni –>RC 23–24/10/2002
Total
WinMx
Http
Dns
KaZaA
ftp
Dns
Http
Netbios
Kazaa
eDonkey
Gnutella
WinMx
Totals
5minBytes
Time
23/10 ore 12:00–24:00
24/10 ore 00:00–12:00


5min–tot- flows per Applicazione Uni –>RC 23–24/10/2002
x 10^4
5minInstances
Time
23:10 ore 12:00–24:00
24:10 ore 00:00–12:00
ftp
Dns
Http
Netbios
Kazaa
eDonkey
Gnutella
WinMx
Totals
Total
Http
WinMx

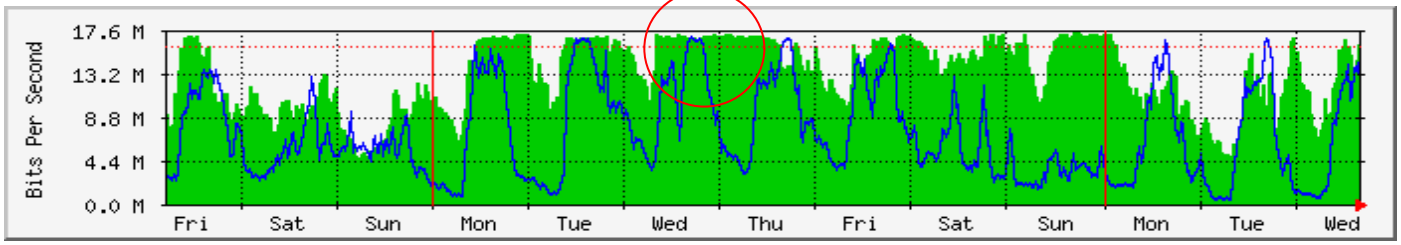
Applicazioni(1)

Comportamenti Anomali

- Pattern di traffico Anomali
- Flash Crowd
- Abusi:
  - DoS
  - Port scans

DoS: un segnale

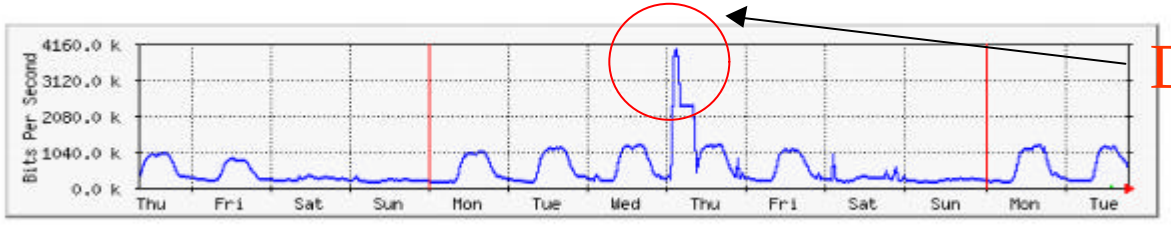
Statistiche MRTG : ATM 34 Mbps



IN

OUT

Statistiche MRTG : Fast Ethernet con soli dati NetFlow relativi al router GARR a cui si attesta il link sopra



DoS

Applicazioni(2)

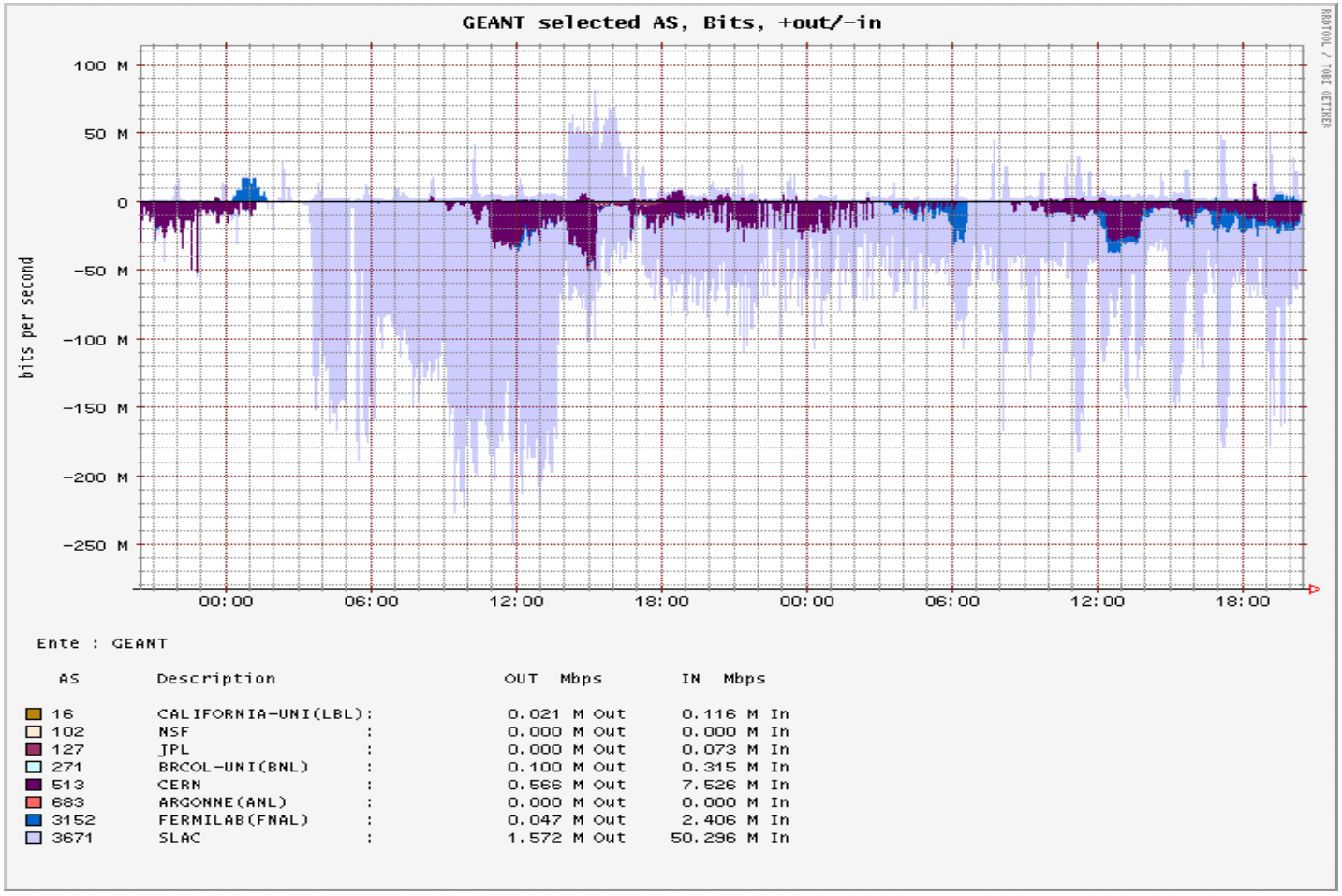
Network Activity

Accounting / Billing

Planning & Analisys

Monitoring / Security

AS-Matrix


GEANT selected AS, Bits, +out/-in
100 M
50 M
0
-50 M
-100 M
-150 M
-200 M
-250 M
bits per second
00:00
06:00
12:00
18:00
00:00
06:00
12:00
18:00
Ente : GEANT
AS Description OUT Mbps IN Mbps
16 CALIFORNIA-UNI(LBL): 0.021 M Out 0.116 M In
102 NSF : 0.000 M Out 0.000 M In
127 JPL : 0.000 M Out 0.073 M In
271 BRCOL-UNI(BNL) : 0.100 M Out 0.315 M In
513 CERN : 0.566 M Out 7.526 M In
683 ARGONNE(ANL) : 0.000 M Out 0.000 M In
3152 FERMILAB(FNAL) : 0.047 M Out 2.406 M In
3671 SLAC : 1.572 M Out 50.296 M In

Riferimenti

http://www.noc.garr.it/fdoc.htm (documento e tutorial GARR)

http://www.splintered.net/sw/flow-tools/

http://net.doit.wisc.edu/plonka/FlowScan/

http://www.rrdtool.org/

http://www.linuxgeek.org/netfow-howto.php

http://www.ietf.org/html.charters/ipx-charter.html

christian.cinetto@garr.it

michele.sciuto@garr.it

noc@garr.it