Utilizzo di strumenti di network accounting a supporto della gestione di infrastrutture complesse

Massimo Ianigro, CNR

Paolo Lucente, CNR

Pisa, 12 Maggio 2005

Network monitoring

Le domande …

- Qual è lo stato attuale della rete?
- Come cambia l’occupazione della banda disponibile?
- Come fluttua il ritardo nella consegna dei dati degli utenti?
- Abbiamo più peerings, quali sono i più utilizzati? Sono ben dimensionati?
- Quali sono le applicazioni/i servizi più usati dagli utenti?
- Si sta diffondendo un worm/virus nella nostra rete?
- Siamo oggetto o stiamo generando un DoS?

Network monitoring

… le risposte dipendono dal tipo di monitoring (I)

Il monitoring attivo (es. ping, traceroute, mping, strumenti client/server) è una sonda introdotta nella rete e ci può dire:

- Quanti pacchetti vanno persi ?
- Quanto tempo impiega la rete a trasportare i pacchetti ? Come varia il ritardo ?
- Quale percorso fanno i nostri pacchetti ? Cosa ne fa la rete del traffico degli utenti ?

Network monitoring

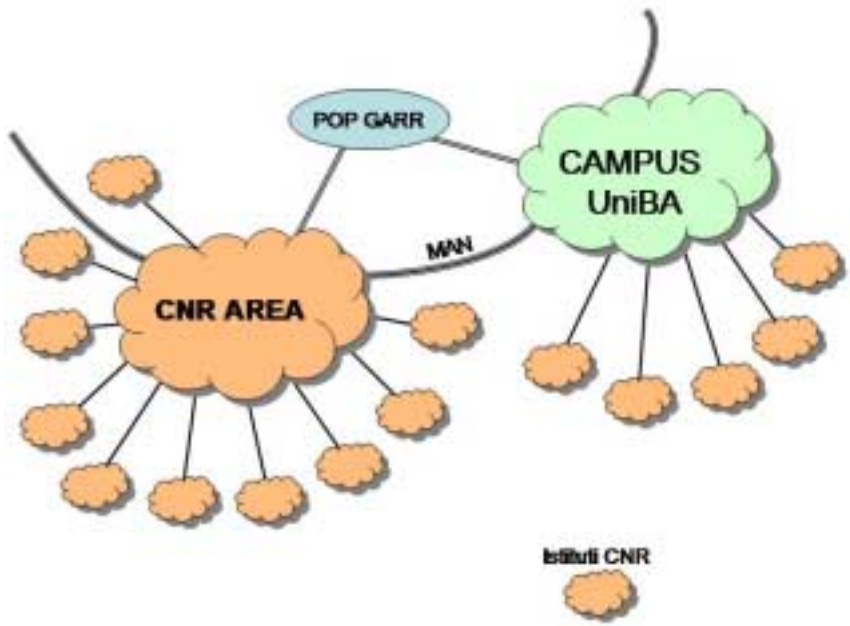
… le risposte dipendono dal tipo di monitoring (II)

Il monitoring passivo (es. snort, ethereal, pmacct, flow-tools, ntop) è un punto di osservazione e ci può dire:

- Come cambia l'occupazione della banda disponibile? Chi sta usando la rete?
- Quali sono le applicazioni/i servizi più usati dagli utenti? Da cosa è composto il mix del traffico di rete?
- Siamo oggetto o stiamo generando un DoS? Si sta diffondendo un virus/worm nella nostra rete?
- Perché, nonostante la nostra rete sia veloce, la mia connessione è così lenta?

Il PoP CNR-BA

La rete del CNR a Bari e i nostri obiettivi (I)



Il PoP CNR-BA

La rete del CNR a Bari e i nostri obiettivi (II)

- Vogliamo generare grafici di occupazione di banda per istituto.
- Vogliamo raccogliere i dati di rete esclusivamente per la generazione di report.
- Vogliamo presentare i dati raccolti ai gestori delle nostre reti, assicurandoci che ognuno di essi possa accedere solo ai propri dati.

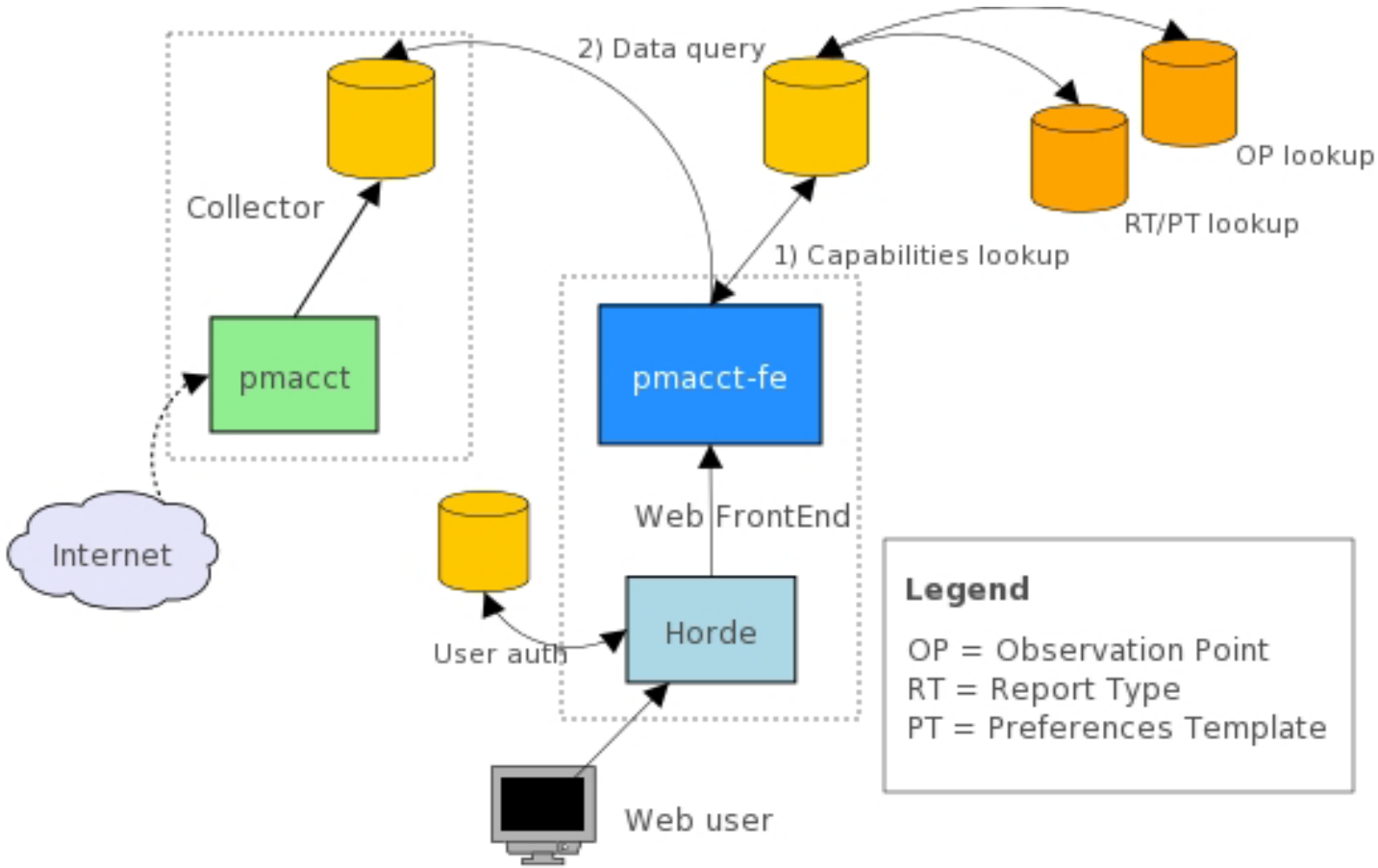
pmacct e pmacct-fe

URL: http://www.ba.cnr.it/~paolo/pmacct/

- ***pmacct*** è un insieme di demoni (pmacctd, nfacctd) per catturare e aggregare traffico IPv4/IPv6. E' in grado di memorizzare gli aggregati in memoria o in un database MySQL/PostgreSQL. Può catturare il traffico via libpcap (per esempio, da una porta di mirroring) o NetFlow v1/v5/v7/v8/v9. **Licenza:** GPLv2.

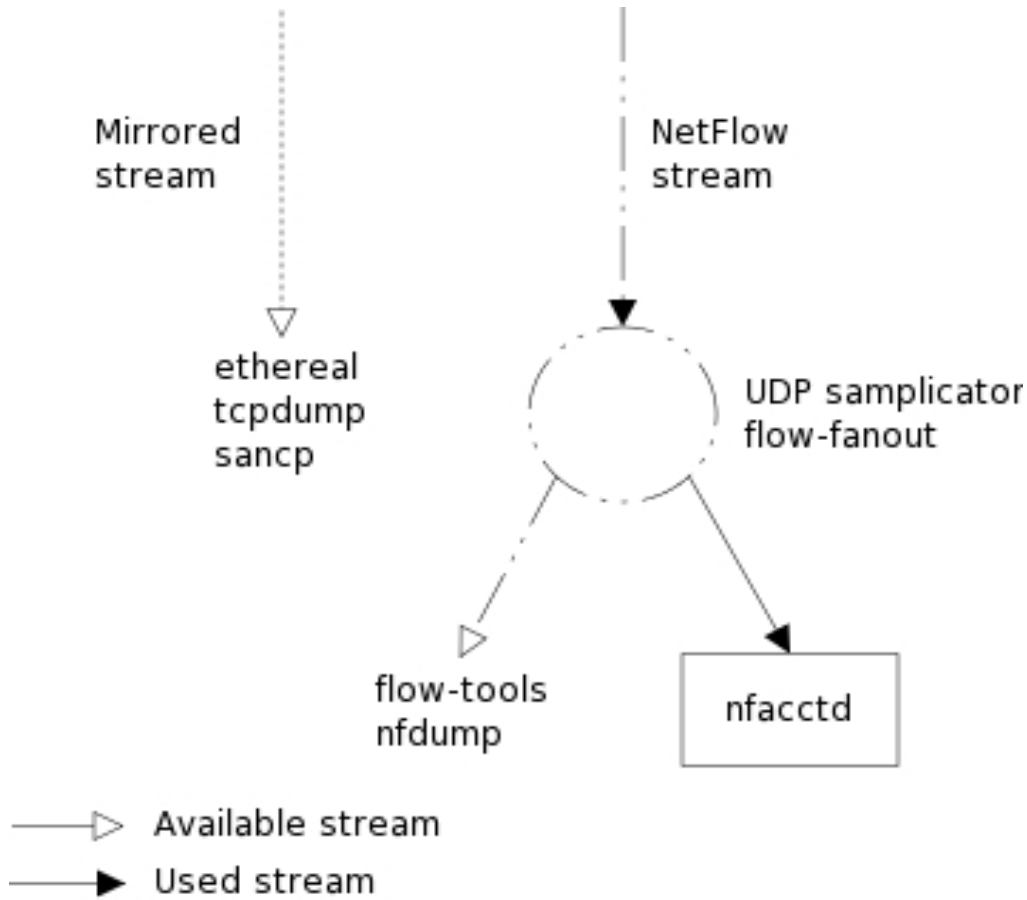
- ***pmacct-fe*** è un tool per la presentazione dei dati raccolti in forma di tavole e grafici. Supporta l'autenticazione degli utenti e l'applicazione di capabilities (cioè ogni utente può accedere solo alle sottoreti di propria competenza). Supporta anche punti di osservazione multipli e report configurabili. **Licenza:** GPLv2.

pmacct e pmacct-fe (II)

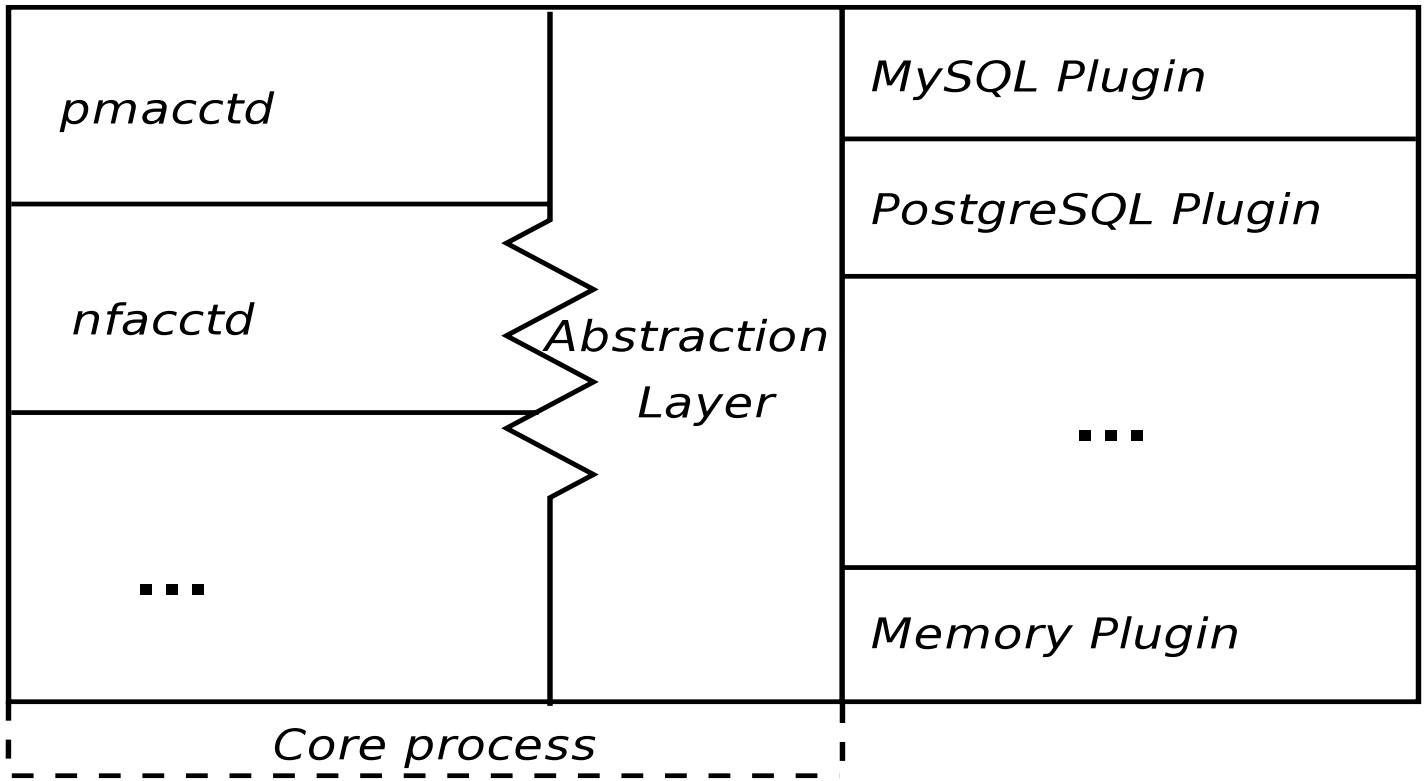


Il PoP CNR-BA

Our deployment

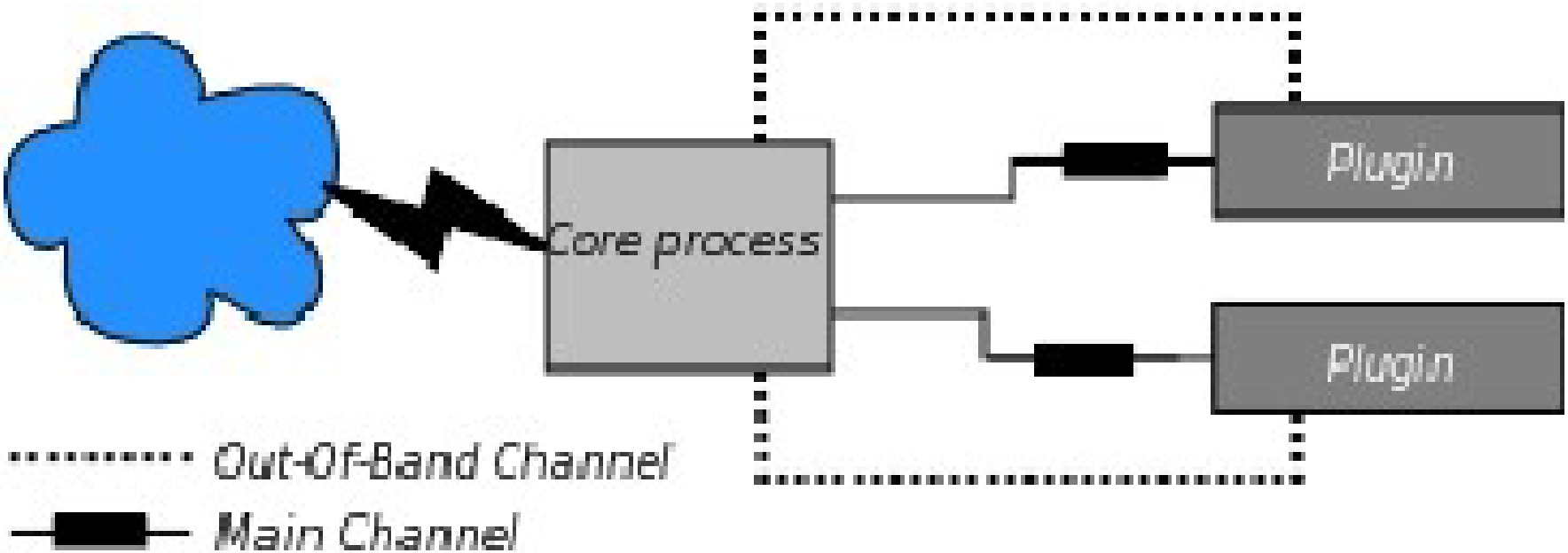


pmacct: cenni sull’architettura (I)



I demoni (*pmacctd* e *nfacctd*) sono divisi in:
- uno strato superiore che cattura i pacchetti/flussi.
- un **Abstraction layer** che semplifica la scrittura di nuovi core processes e plugins.
- uno strato inferiore, i **Plugins**, che interagisce con i backends.

pmacct: cenni sull’architettura (II)

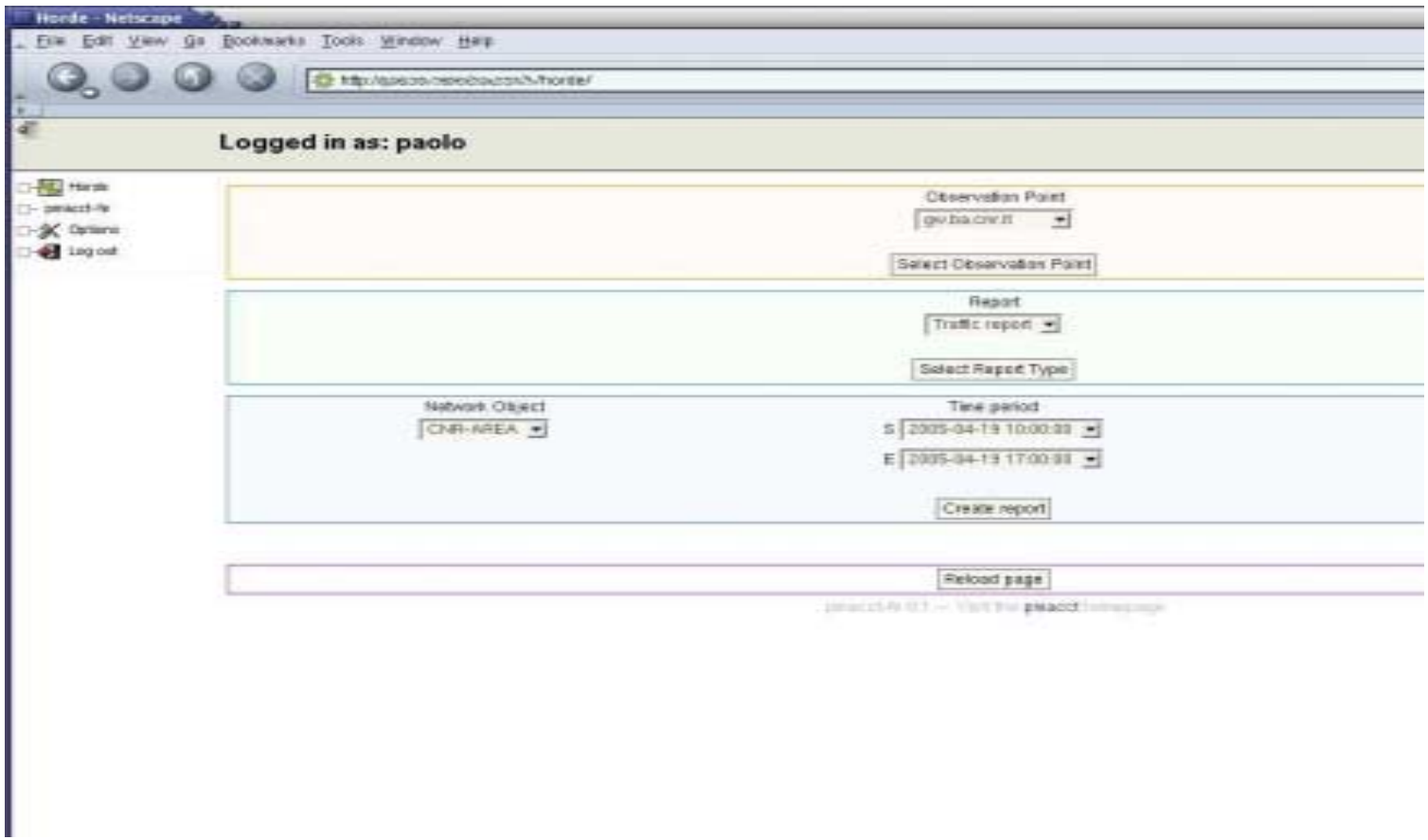


La comunicazione tra **Core process** e **Plugins** attivati è basata su:

- Un canale principale in cui vengono copiati i dati.
- Un canale di segnalazione fuori banda per la notifica dell’arrivo di nuovi dati.

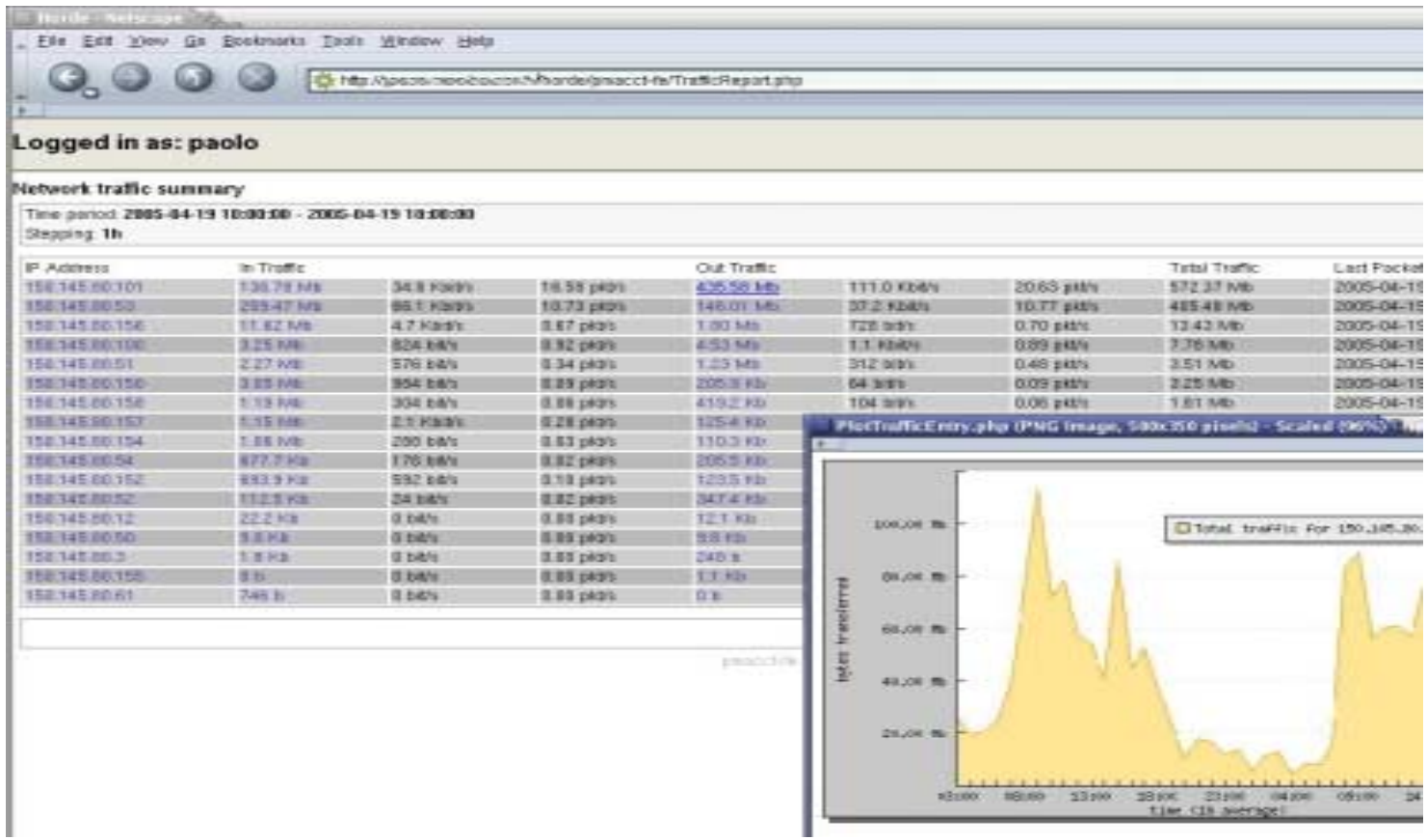
Il PoP CNR-BA

I risultati (I)



Il PoP CNR-BA

I risultati (II)



Il PoP CNR-BA

Alcune note finali: analisi del traffico del PoP

- Caccia agli “elefanti”: un semplice meccanismo di notifica nel caso di occupazione di banda eccessiva da parte di uno stesso IP e per un tempo prolungato.
- Caccia alle “formiche”: sulle tracce di scansioni di porte, scansioni del pool di IP e replicazione di worms.
- Alcune idee su network monitoring e traffico P2P.

Grazie per l’ascolto.
Annoiati? Domande?

Massimo Ianigro
ianigro@ba.issia.cnr.it

Paolo Lucente
lucente@area.ba.cnr.it