# ntop: Monitoraggio di Rete Open Source

*Open Source Conference 2013*

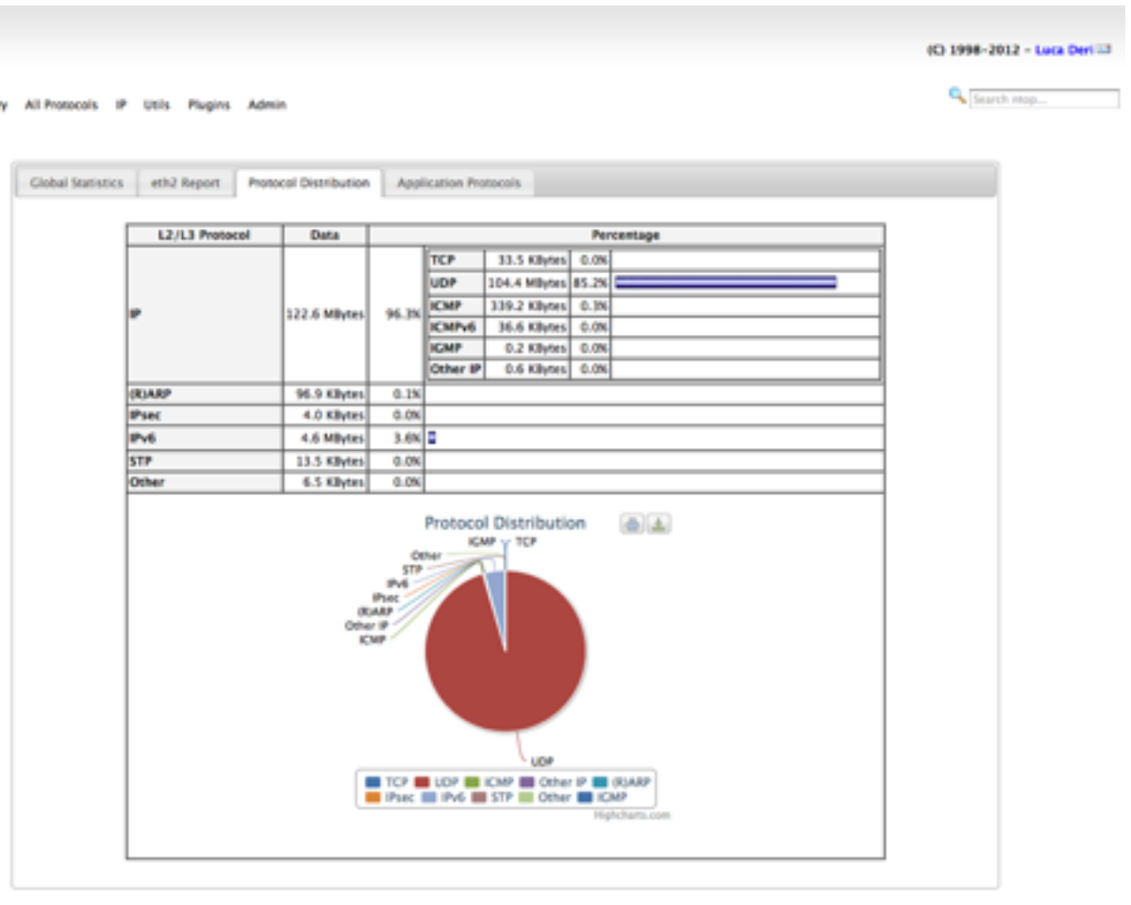
Luca Deri <deri@ntop.org>

# Cosa Presenterò in Questo Intervento

- Quello che ntop fa, e come potete utilizzare il software open-source che sviluppiamo.
- Come si riesce a migliorare la visibilità di rete utilizzando il DPI (Deep Packet Inspection).
- Perchè la correlazione in real-time del traffico di rete tramite una "network knowledge cloud database" permette di conoscere meglio quello che accade nella nostra rete.

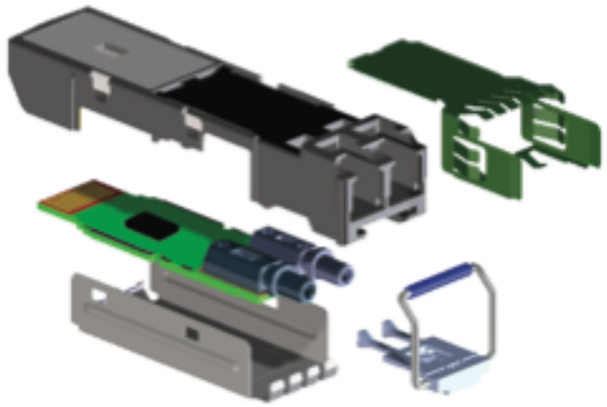
# Cosa fa ntop ? [1/3]

- Ditta privata che opera nel settore del monitoraggio di rete utilizzando strumenti open-source sviluppati nel corso degli anni.
- ntop è stata la prima applicazione rilasciata (1998) finalizzata al web-based network monitoring.



# Cosa fa ntop ? [2/3]

- Il nostro software è presente in molti prodotti commerciali...



Integrated ASIC with JDSU technology


WÜRTHPHOENIX

# Cosa fa ntop ? [3/3]

- ...e vi permettiamo di inviare/ricevere traffico a 1/10 Gbit (any packet size) senza perdita utilizzando schede di rete commerciali.
- Quindi non acceleriamo solo le nostre applicazioni ma anche molte altre applicazioni.





# Oltre le Intestazioni dei Pacchetti

- Tradizionalmente le applicazioni di monitoraggio limitano la loro analisi alle intestazioni dei pacchetti di rete:
  - Port 80a = HTTP.
  - La rete x.y.z.0/24 identifica la sede di Roma.
  - TCP:443 è una connessione sicura (HTTPS).

- Purtroppo quanto sopra non è più vero:
  - I protocolli possono utilizzare porte dinamiche.
  - "Well known ports" possono essere utilizzate per traffico che non aspetteremo di avere in rete (80 != http).
  - Encryption non è sempre sinonimo di sicurezza (SSL vs OpenVPN).

# L'uso del DPI nel Monitoraggio [1/2]

- Limitare l'analisi del traffico di rete alle intestazioni dei pacchetti non è più sufficiente (nè una buona idea perchè può trarci in inganno).
- Gli amministratori di rete vogliono conoscere il vero protocollo di rete senza conoscere la porta effettivamente utilizzata.
- Alcuni protocollli (es. HTTP) possono essere analizzati in dettaglio per raccogliere metadati (es. User-Agent) utilizzati per ricavare informazioni ulteriori (es. sistema operativo).

# L'uso del DPI nel Monitoraggio [2/2]

- DPI (Deep Packet Inspection) è una tecnica di analisi del contenuto del pacchetto finalizzata al riconoscimento del protocollo ed estrazione di metadati.
- Esitono toolkit DPI sul mercato ma non vanno bene:
  - Sono proprietary(occorre firmare una NDA per usarli), son costosi sia per il prezzo che per la manutenzione (che poi inevitabilmente pagano utenti finali).
  - Non è tipicamente possibile aggiungere nuovi protocolli senza che lo faccia il produttore del toolkit DPI: l'utente è in gabbia.
- In sostanza il DPI è oggi un componente necessario, ma il mercato non offre alternative al mondo dell'open-source.

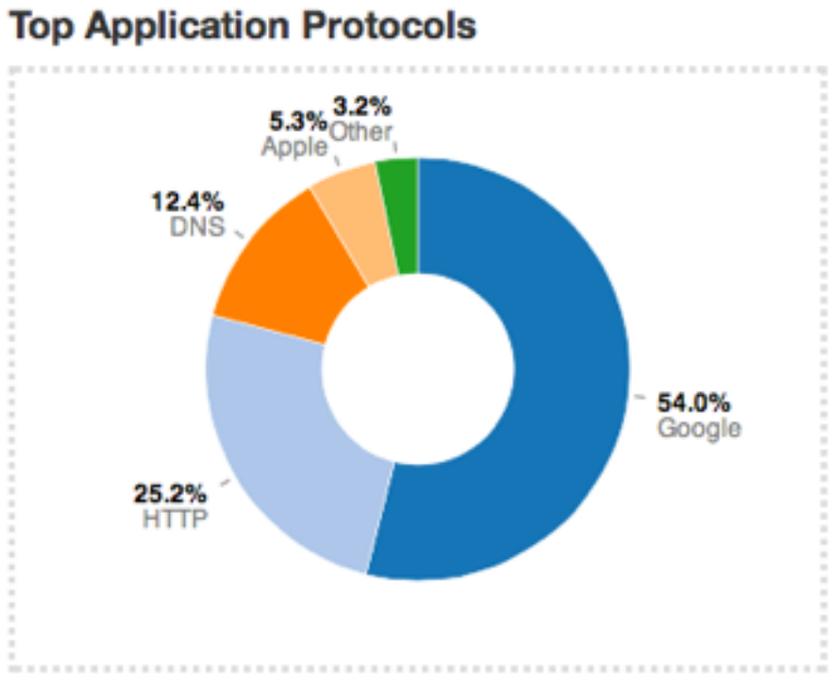
# Benvenuto nDPI

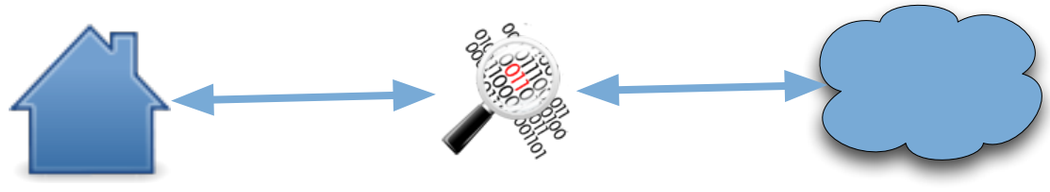
- ntop ha deciso di sviluppare il suo toolkit di DPI chiamato nDPI in modo da avere una libreria GPL DPI che possa essere usata sia nelle applicazioni di ntop che in quella di terze parti senza costi aggiuntivi per l'utente finale.
- I protocolli attualmente supportati (~170) includono:
  - P2P (Skype, BitTorrent)
  - Messaging (Viber, Whatsapp, MSN, The Facebook)
  - Multimedia (YouTube, Last.gm, iTunes)
  - Conferencing (Webex, CitrixOnLine)
  - Streaming (Zattoo, Icecast, Shoutcast, Netflix, Spotify)
  - Business (VNC, RDP, Citrix, *SQL)

OpenDPI.org

# Cosa si Riesce a fare con nDPI?

- Riconoscere e catalogare (es. con NetEye) i protocolli effettivamente presenti in rete.
- Bloccare comunicazioni di rete application firewall (PaloAlto-like). Questo prodotto è attualmente sotto test e sarà presto disponibile su Linux.

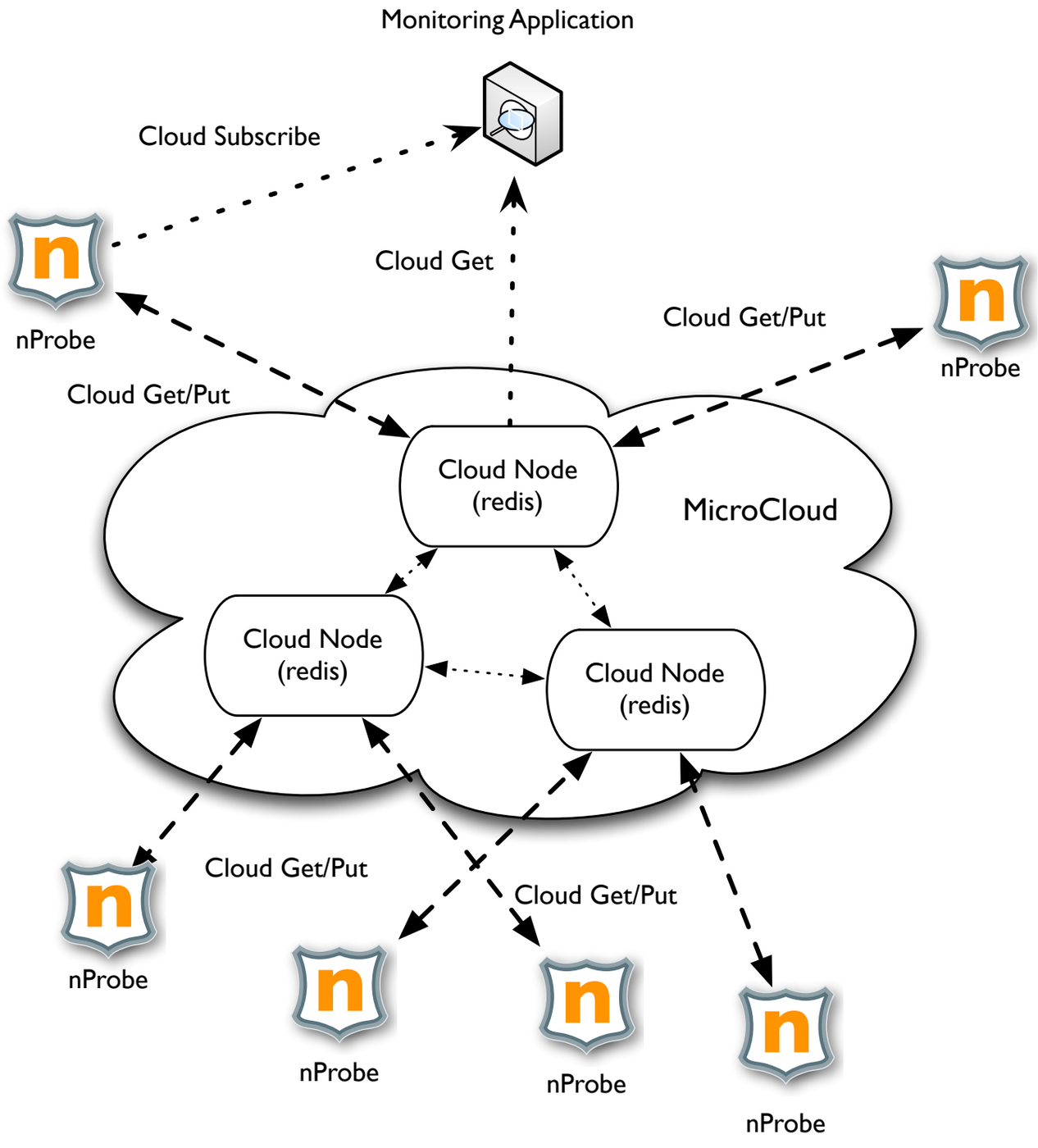


# We Need The Big Picture. In Realtime.

- nDPI è una ottima soluzione per vedere quello che passa in rete a livello di connessione.
- La correlazione di traffico (es. segnalazioneVoIP con la voce) è una cosa che tipicamente le applicazioni di monitoraggio non fanno, o fanno usando cluster di databases.
- Gli utenti vogliono avere soluzioni che permettano di vedere cosa accade in rete quando questo accade senza latenza (5 minuti o oltre usate in molti prodotti applicativi).

# MicroCloud: Correlazione in Realtime



# Applicazioni del MicroCloud

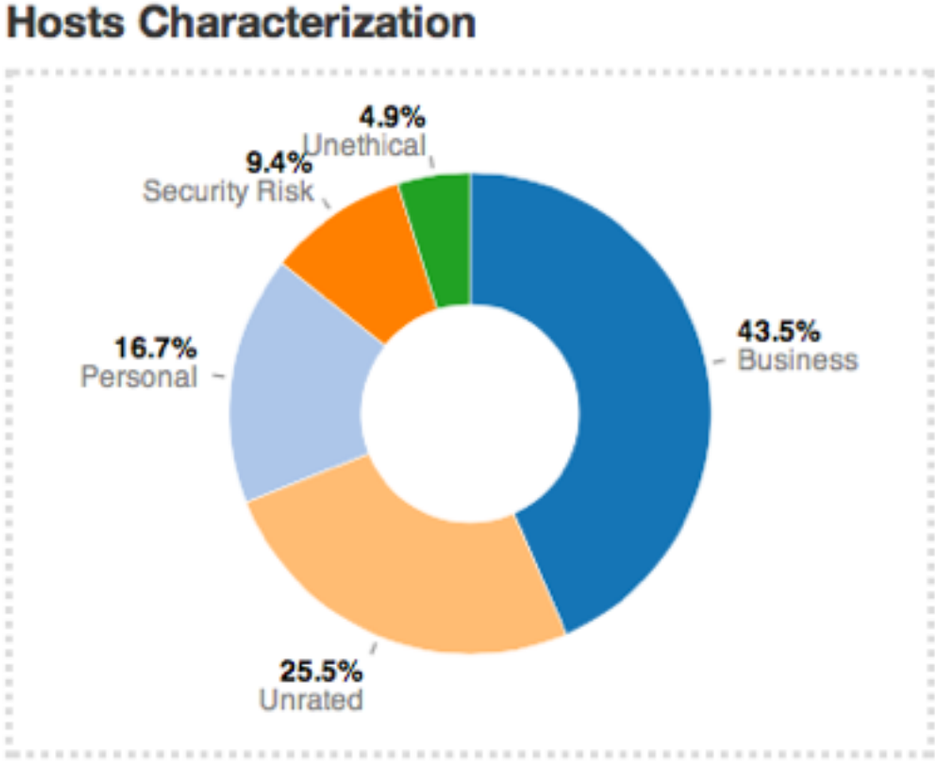
- Associare un numero di telefono VoIP alla chiamata ancora in corso per vedere in tempo reale il suo stato.
- Memorizzarvi i dati utente (es. Radius IP/User/IMSI/MSISDN) in modo che le sonde di rete possano inviare alle console di monitoraggio (es. NetEye) i nomi degli utenti e non i loro IP che non sono permanenti.
- Creare una federazione di applicazioni (e.g. IDS, network probes, firewall logs) in modo da avere una vista realtime della rete: la "reputazione" di un host è la "sintesi" della sua reputazione cosí come vista da tutti i componenti di rete.

# Quale Sarà il Prossimo Passo?

- I report di traffico sono ancora troppo complessi. DPI ha permesso di avere maggiore precisione nei dati visualizzati, eliminando incertezze sui protocolli.
- I gestori di rete, ma anche "chi paga Internet ai propri dipendenti" vuol sapere, come viene usato il traffico di rete: piacere o lavoro?
- È tempo di pensare a nuovi report di traffico, molto aggregati e quindi sintetici, che sintetizzino come viene usata la rete.

# Categorizzazione del Traffico

- Immaginate di avere un sistema che categorizzi ogni sito Internet indicando la sua tipologia (es. notizie, viaggi, business).
- Immaginate di integrarlo nelle sonde di rete per avere un ulteriore visibilità.
- ntop e blocksi hanno reso questo possibile nelle proprie sonde di rete open source.



# Conclusioni

- DPI è il primo passo per promuovere la visibilità di quello che accade veramente in rete.
- Microcloud permette di correlare informazioni di rete (es. utenti) e traffico in realtime, mentre questo accade.
- La categorizzazione dei siti Internet permette di estendere ulteriormente questa visibilità in modo da offrire un nuovo tipo di visualizzazione del traffico di rete.

# Referenze

- Web Site: http://www.ntop.org
- Blog: http://blog.ntop.org
- Software: http://packages.ntop.org