

# Gestione di Rete

Luca Deri  
[deri@ntop.org](mailto:deri@ntop.org)  
[luca.deri@di.unipi.it](mailto:luca.deri@di.unipi.it)

# Riferimenti [1/2]

# Slides Corso: MS Teams

<http://luca.ntop.org/>

Indirizzo Email: [deri@ntop.org](mailto:deri@ntop.org)

luca.deri@di.unipi.it

# Aula Ricevimento: TBD

Orario Lezioni: Lunedì Aula LI 9.00-10.45  
Martedì Aula MI 9.00-10.45

# Riferimenti [2/2]

Progetti: <https://github.com/lucaderi/sgr>  
Gruppo Telegram: <https://t.me/gestionedirete>



# Panoramica del Corso

- Introduzione ai principali protocolli per il monitoraggio di rete.
- Conoscenza pratica di alcuni casi comuni di monitoraggio e loro risoluzione.
- Panoramica sullo stato dell'arte inclusi gli sviluppi attuali e le ricerche in corso.
- Cybersecurity ed Analisi Dati.
- Questo non è un corso solamente teorico.

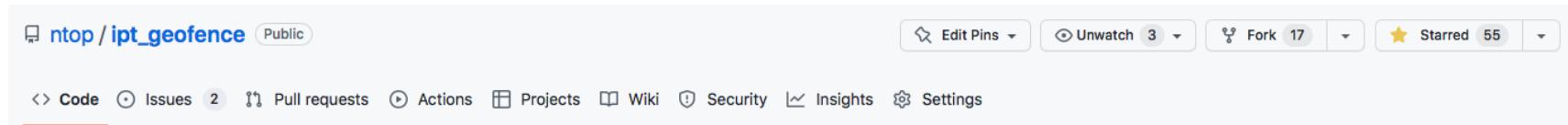
# Obiettivi del Corso

- Dare una conoscenza ‘pratica’ della materia estendendo conoscenze di reti esistenti.
- Risolvere assieme problemi comuni di monitoraggio e sicurezza.
- Fare capire cosa succede ‘veramente’ nei sistemi di comunicazione (dalla interfaccia utente al cavo di rete).
- Analizzare i dati raccolti tramite algoritmi di analisi numerica in modo da capire veramente cosa succede in rete.

# Prerequisiti

- Conoscenza *minima* di come funziona una rete Internet.
- Volontà di imparare come funzionano nella pratica i sistemi di comunicazione.
- Interesse a ‘volersi sporcare le mani’ a programmare nuovi strumenti per l’analisi accurata del traffico di rete.

# Modalità di Esame



- Breve progetto pratico da realizzare da soli o in coppia e da consegnare su GitHub.
- Orale prevalentemente sulla parte del corso orientata alla misura del traffico di rete.

# <https://github.com/lucaderi/sgr>

The screenshot shows the GitHub repository page for `lucaderi/sgr`. The repository is public and has 599 commits. The README.md file contains the following content:

```
Progetti Corso Gestione di Rete

Questa cartella contiene i progetti studenti del corso di Gestione di Rete (vecchio nome SGR)
```

The repository has 84 forks, 10 stars, and 1 watching. It uses the C language (49.5%), HTML (11.3%), C++ (7.6%), Python (6.2%), Java (5.2%), Shell (5.1%), and Other (15.1%).

# Supervisione Tesi

- Disponibile a fare da supervisione tesi di laurea su argomenti attinenti a questo corso (networking, analisi dati, cybersecurity).
- Potete trovare alcune tesi “generiche” disponibili sul portale del dipartimento.
- Le tesi sono la **conclusione** del vostro percorso di studio e quindi devono essere il più possibili vicine ai vostri interessi: per questo meglio non fare tesi “generiche” ma concordare i contenuti assieme.

# Motivazione [1/2]



“Without data  
you’re just  
another person  
with an opinion.”

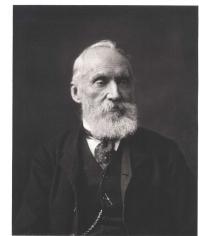
- W. Edwards Deming,  
Data Scientist

# Motivazione [2/2]

- Senza misure non possiamo produrre i risultati attesi, misurare i miglioramenti e quantificare il successo.
- Il traffico di rete non fa eccezione a questa regola.

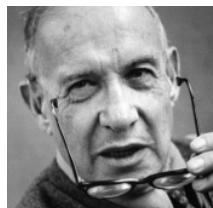
If you can't measure it, you can't improve it

(Lord Kelvin, 1824 – 1907)



© Wikipedia/Albert R. Stone

Lord Kelvin

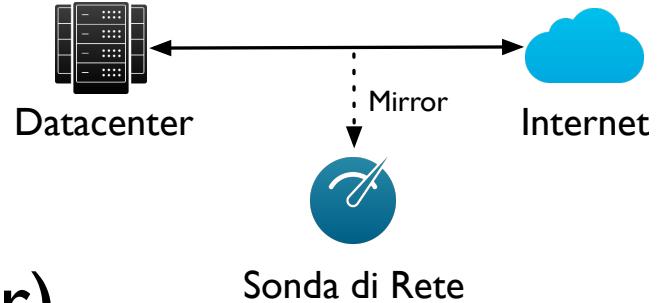


If you can't measure it, you can't manage it

(Peter Drucker, 1909 – 2005)

# Come si Misura il Traffico di Rete

1. Individuare un punto della rete dove passa il traffico da analizzare (tipicamente vicino al router).
3. Installazione di una sonda di rete capace di analizzare tale traffico:
  1. Passiva: solo analisi, no modifica/blocco traffico.
  2. Attiva: il traffico attraversa la sonda che può bloccarlo se necessario.



# Che Misure di Rete Possiamo Fare?

- **Analisi Quantitativa di Traffico**
  - Top Talkers (Senders and Receivers)
  - Destinazioni verso/da le quali viene scambiato traffico.
  - Protocolli applicativi utilizzati (Skype, HTTP, Email)
  - Rendicontazione traffico per host.
- **Analisi Qualitativa di Traffico**
  - Utilizzo di traffico non permessi (es. Tor o VPN anonime).
  - Identificazioni errori ed anomalie di rete che possono causare malfunzionamenti nell'utilizzo dei servizi di rete.

# Didattica

- Introduzione
- *Monitoraggio di reti Ethernet/IP*
- Introduzione alla misurazione del traffico di rete.
- Configurazione ed utilizzo pratico di router e sistemi di monitoraggio per piccole reti
- Strumenti open-source per il monitoraggio di rete e la risoluzione di comuni problemi di rete.
- *Misure utilizzando soluzioni basate SNMP.*
- *Flow-based Measurement: NetFlow/IPFIX, sFlow.*
- Misurazione di Rete: casi reali di monitoraggio.
- Analisi del traffico di rete orientato alla **cybersecurity**.
- Memorizzazione ed analisi delle misure di rete in serie temporali (timeseries).
- *Deep packet inspection (DPI) per la caratterizzazione del traffico di rete applicativo.*
- Monitoraggio degli eventi di sistema utilizzando eBPF.
- Cattura e gestione di traffico ad alta velocità
- *Algoritmi per l'analisi dei dati di traffico*

## Note

- In *italico* gli argomenti che fanno parte dell'esame del corso.
- Tra tali argomenti alcune parti sono escluse.

# Parte Pratica ed Esercitazioni

- Wireshark (Analisi Pacchetti di Rete)
- RRD (Round Robin Database)
- nDPI (Deep Packet Inspection)
- Analisi dati di rete

# Nuovi Argomenti

- Analisi traffico orientato alla Cybersecurity
- Algoritmi per l'analisi dei dati del traffico di rete.
- Traffic fingerprinting
- Utilizzo AI/ML nell'analisi del traffico di rete
- Rilevazione Anomalie
  - Analisi serie temporali
  - Indicatore di comportamenti inaspettati
  - Utilizzo di tecniche per la rilevazione di anomalie
  - Analisi statistica vs Machine Learning

# Obiettivo Finale: Visibilità e Sicurezza

Aggregated 520.70 Mbps 104.80 Mbps 2K 29.9K 3.1K 2.8K (91) 41.3K (4.3G) 199.7K

2 K Engaged Alerts 3 K Active Hosts 199 K Active Flows

Interfaces Traffic

Aggregated - Sent Aggregated - Rcvd tcp://127.0.0.1:17901c - Sent tcp://127.0.0.1:17901c - Rcvd tcp://127.0.0.1:17900c - Sent tcp://127.0.0.1:17900c - Rcvd

Top Local Hosts

Host	Current Traffic
	372.50 Mbps
	185.90 Mbps
	159.60 Mbps
	152.70 Mbps
	143.20 Mbps
	122.00 Mbps

Top Remote Hosts

Host	Current Traffic
	69.80 Mbps
	46.60 Mbps
	44.90 Mbps
	20.70 Mbps
	12.90 Mbps
	11.50 Mbps

Top Applications

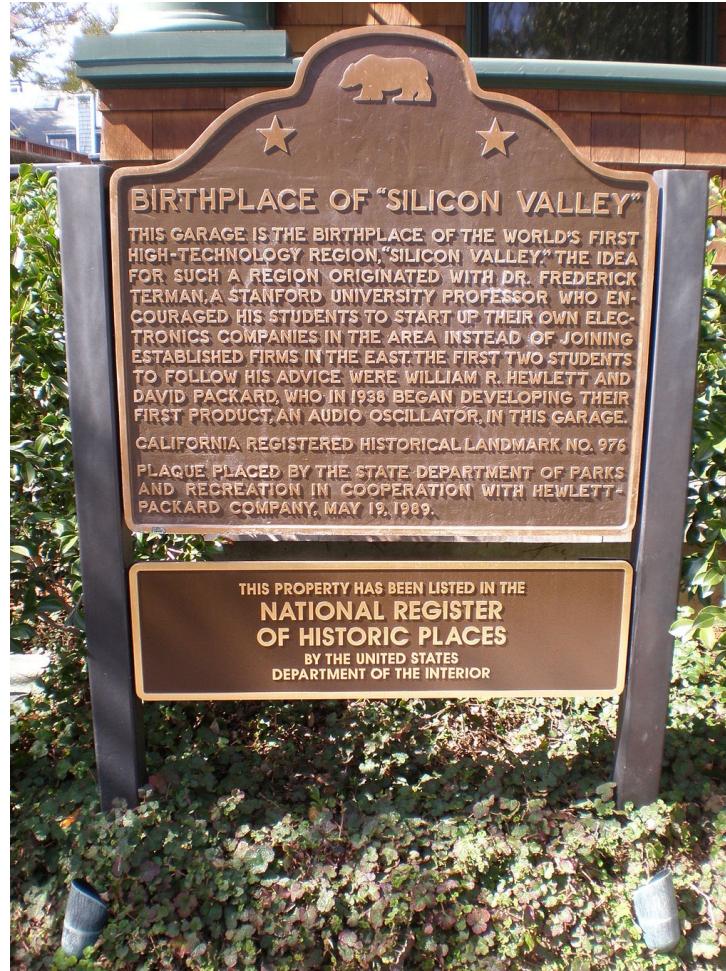
Application	Percentage
DNS	28.0%
TLS	22.1%
RDP	19.1%
HTTP	7.9%
Cybersec	3.5%
Other	19.5%

17

# Nuovo Obiettivo Finale per il 2026

- Sapere rispondere alle seguenti domande
  - Cosa è cambiato oggi nella mia rete?
  - Perché questo host è sospetto?
  - Mostrami traffico simile a questo
  - Cosa c'è di nuovo rispetto alla settimana scorsa?

# Prima di iniziare... [1/3]



# Prima di iniziare... [2/3]



Vala Afshar @ValaAfshar · 9h

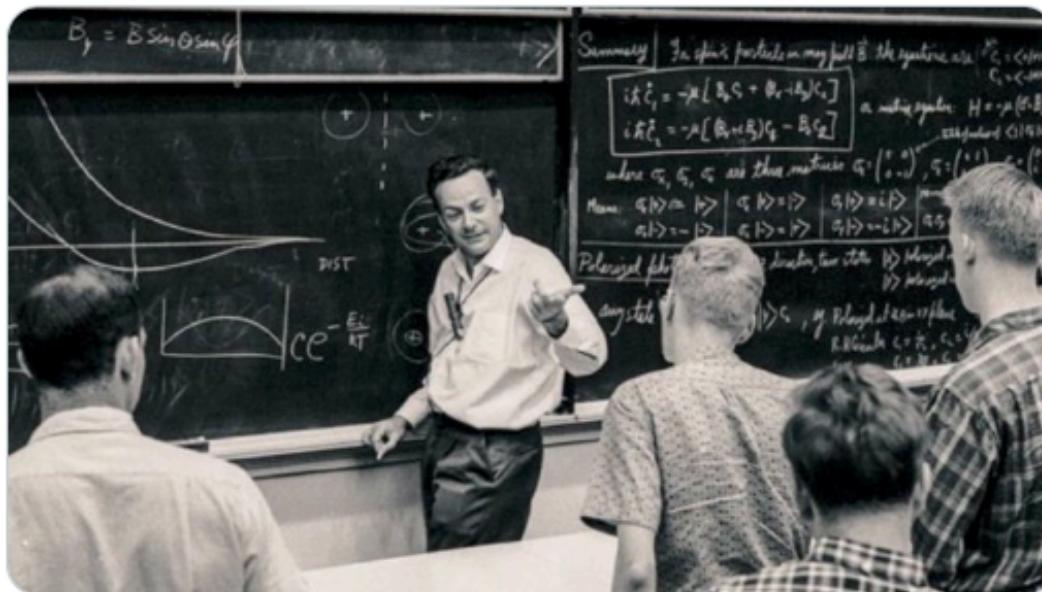
Never confuse education with intelligence.

...

Intelligence isn't the ability to remember and repeat, like they teach you in school.

Intelligence is the ability to learn from experience, solve problems, and use our knowledge to adapt to new situations.

—Professor Richard Feynman



# Prima di iniziare... [3/3]

