

Gestione di Rete

Luca Deri
deri@ntop.org
luca.deri@di.unipi.it

Riferimenti

Slides Corso: MS Teams e <http://luca.ntop.org/>

Indirizzo Email: deri@ntop.org

luca.deri@di.unipi.it

Aula Ricevimento: 372

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

Gruppo Telegram: <https://t.me/gestionedirete>

Orario Lezioni: Lunedì Aula MI 14.00-15.45

Venerdì Aula CI 9.00-10.45

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 é un corso solamente teorico.

Obiettivi del Corso

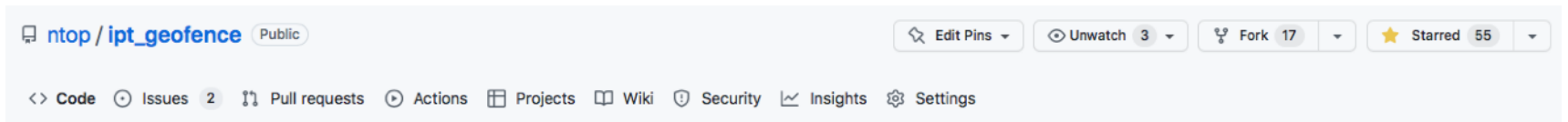
- Dare una conoscenza 'pratica' della materia estendendo conoscenze di reti esistenti.
- Risolvere assieme problemi comuni di monitoraggio e sicurezza.
- Fare capire cosa succede 'veramente' nei sistemi di comunicazione (dalla interfaccia utente al cavo di rete).
- Analizzare i dati raccolti tramite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

- Esercizi “in itinere” sugli argomenti trattati (no compitiini).



- 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

Search of jump to... Pull requests Issues Marketplace Explore

lucaderi / sgr Public Unpin Unwatch 1 Fork 84 Star 10

<> Code Issues Pull requests 1 Actions Projects Wiki Security Insights Settings

master 1 branch 0 tags Go to file Add file Code

File	Description	Commit
2001-2010	Import project 2001-2010	4 years ago
2011-2020	Raggruppamento progetti	20 seconds ago
2021	Bump numpy from 1.20.3 to 1.21.0 in /2021/Lencioni (#219)	22 days ago
.gitignore	Aggiunto .gitignore	4 years ago
README.md	Readme del repository progetti	4 years ago

lucaderi Raggruppamento progetti 27fb6c6 20 seconds ago 699 commits

2001-2010 Import project 2001-2010 4 years ago

2011-2020 Raggruppamento progetti 20 seconds ago

2021 Bump numpy from 1.20.3 to 1.21.0 in /2021/Lencioni (#219) 22 days ago

.gitignore Aggiunto .gitignore 4 years ago

README.md Readme del repository progetti 4 years ago

README.md

Progetti Corso Gestione di Rete

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

About

Progetti Corso Gestione di Rete

[didattica.di.unipi.it/laurea-in-informati...](#)

monitoring network snmp traffic

Readme

10 stars

1 watching

84 forks

Releases

No releases published

[Create a new release](#)

Packages

No packages published

[Publish your first package](#)

Contributors 95

+ 84 contributors

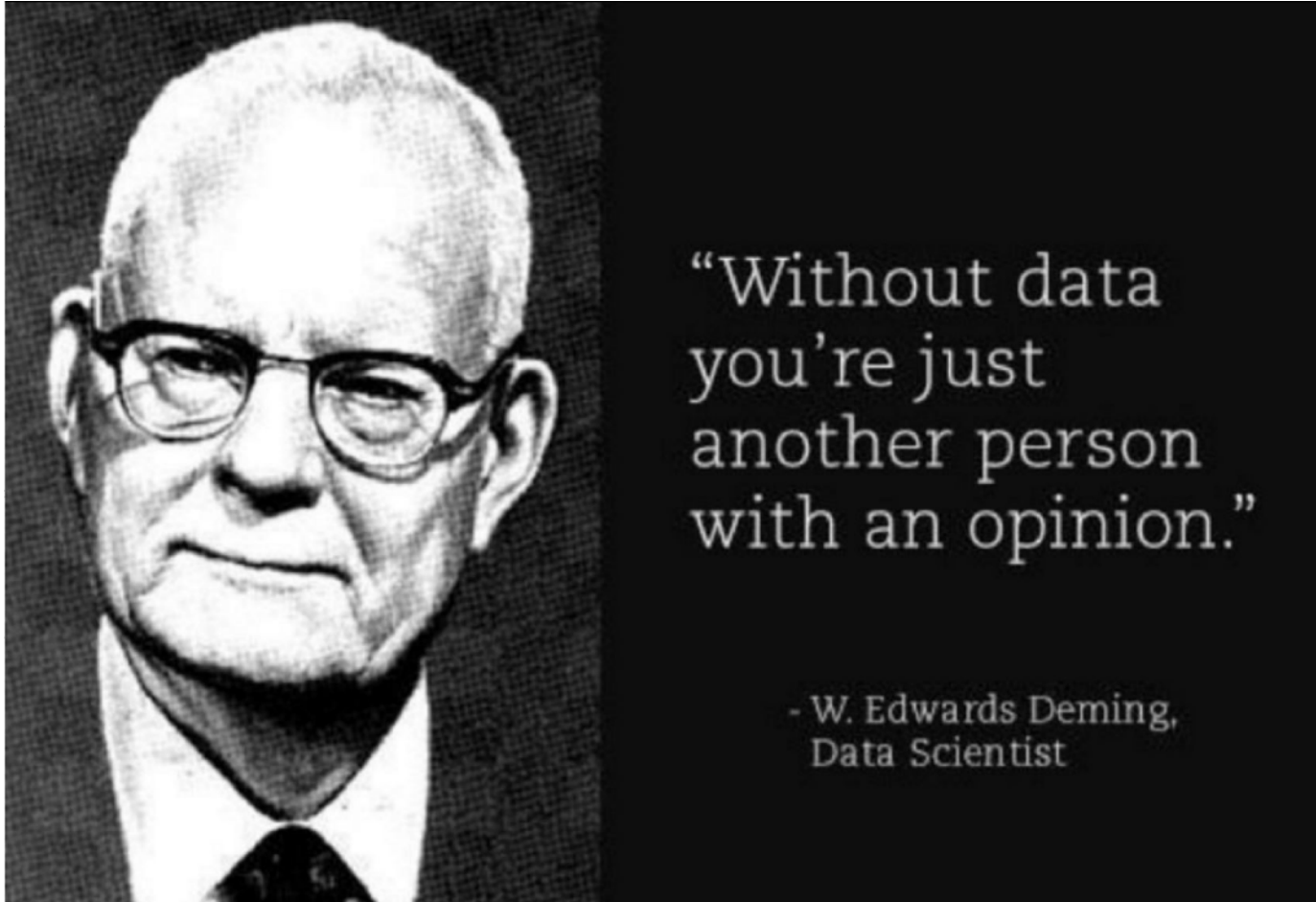
Languages

- C 49.5%
- C++ 7.6%
- Java 5.2%
- HTML 11.3%
- Python 6.2%
- Shell 5.1%
- 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 possibile vicine ai vostri interessi: per questo meglio non fare tesi “generiche” ma concordare i contenuti assieme.

Motivazione [1/2]

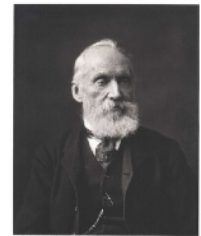


Motivazione [2/2]

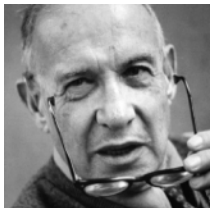
- Senza misure non possiamo produrre i risultati attesi, misurare i miglioramenti e quantificare il successo.
- Il traffico di rete non fa eccezione a questa regola.

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

(Lord Kelvin, 1824 – 1907)



Portrait of Lord Kelvin

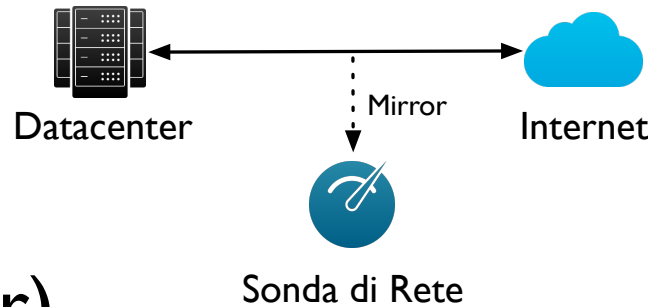


If you can't measure it, you can't manage it

(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.

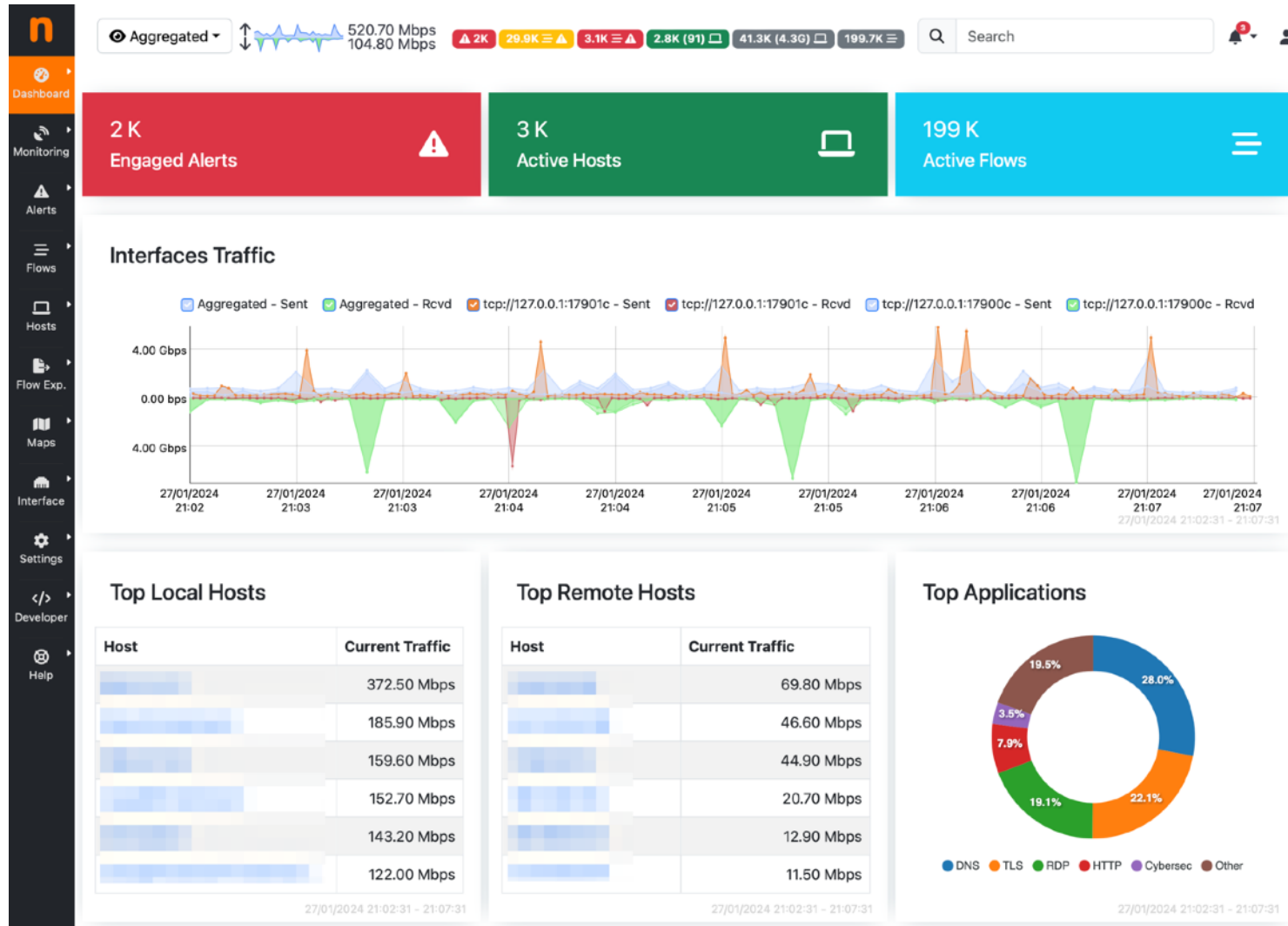
Parte Pratica ed Esercitazioni

- 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
- 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



Prima di iniziare... [1/3]



Prima di iniziare... [2/3]



Vala Afshar ✓ @ValaAfshar · 9h

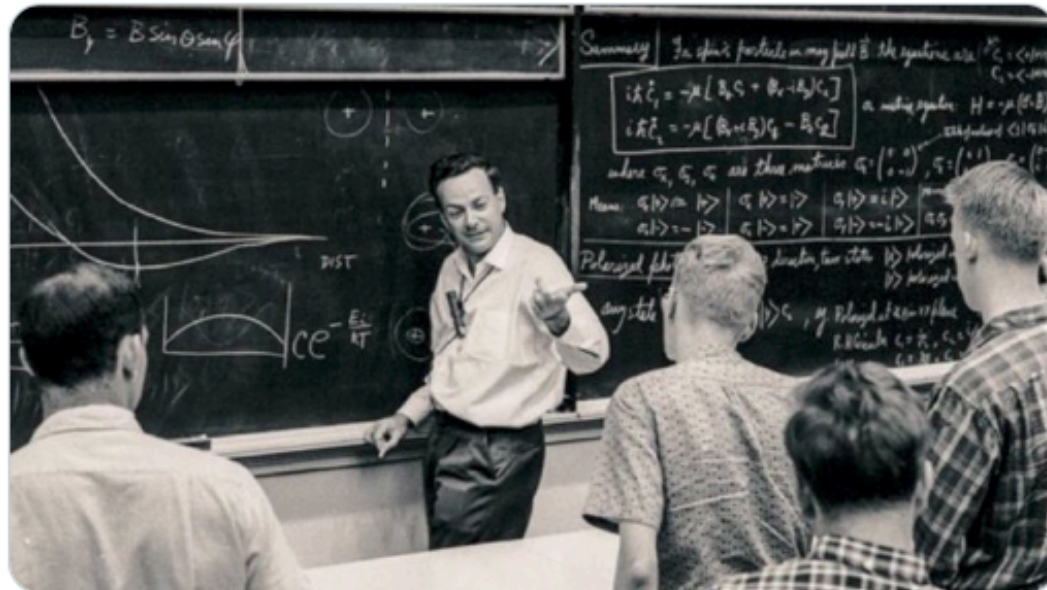
...

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]

