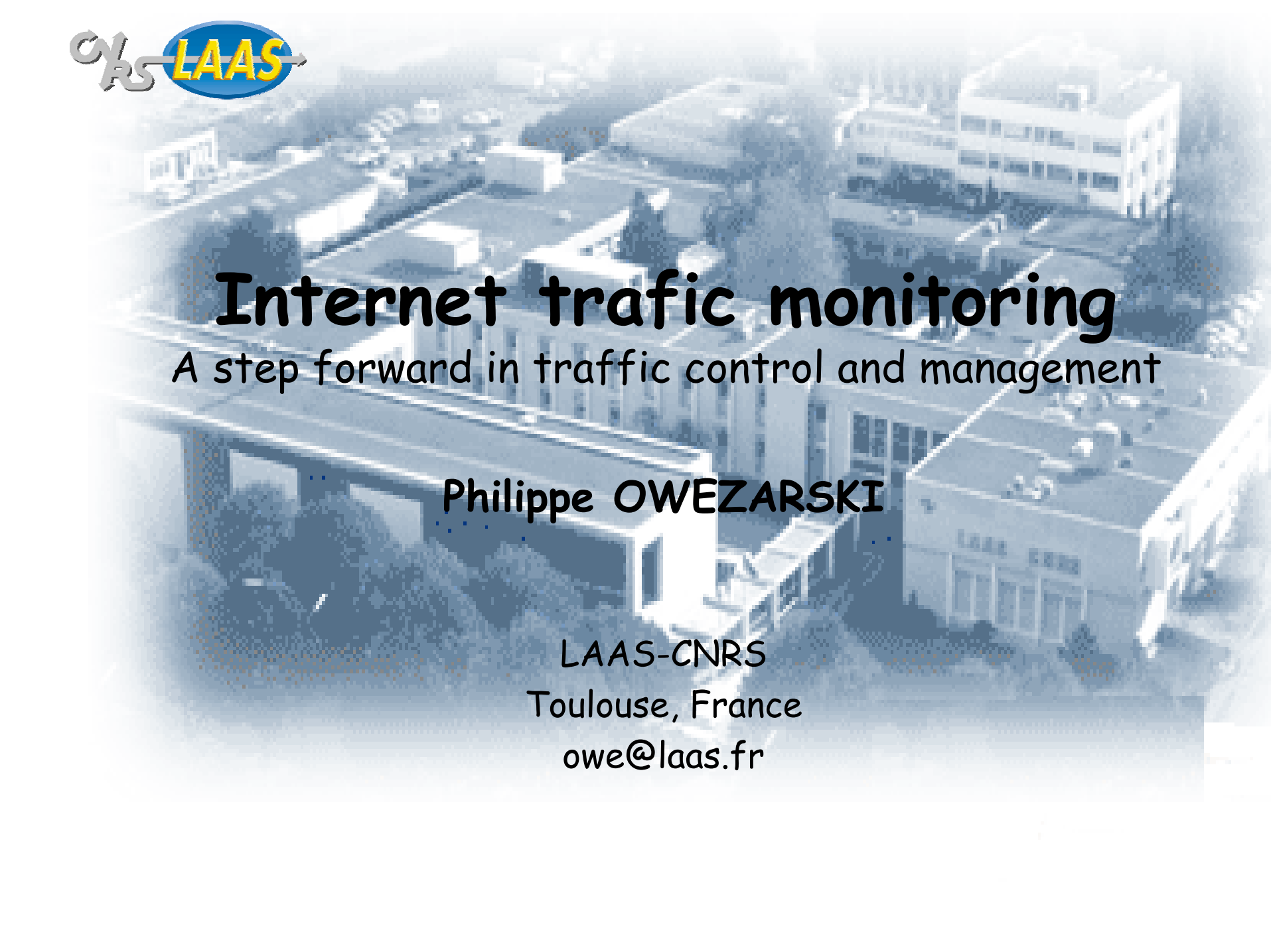


Internet trafic monitoring

A step forward in traffic control and management

Philippe OWEZARSKI

LAAS-CNRS
Toulouse, France
owe@laas.fr

Outline

- Active vs. Passive measurements
- Internet traffic characterization and QoS issue analysis (oscillations & LRD)
- Illustration on a case study: comparison of TCP vs TFRC impacts on traffic oscillations
- Example of a DoS attack characteristics
- A measurement based approach for trafic control and management
- Conclusion

Active measurements

- Active measurements
  - Consists in sending packets on a network and observing results (Delay, RTT, Throughput, etc.)
  - User point of view
  - Best solution to evaluate the service you can get from the network you're connected to
- Drawbacks
  - Probe packets change the state of the network (can be seens as an attack)

    →IETF IPPM WG is working on the definition of probing scenarios minimizing the effects on the network state

Passive measurements

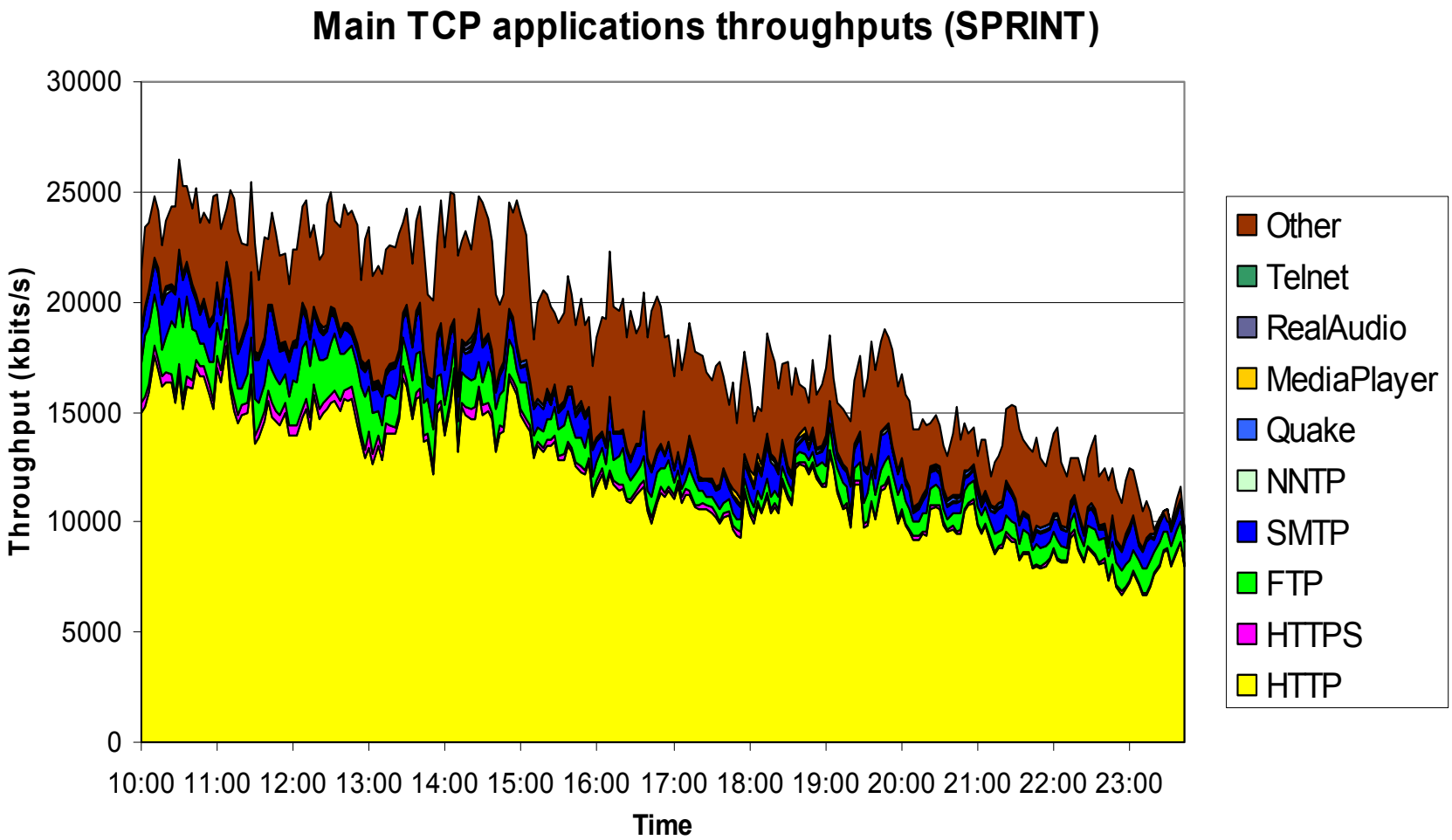
- Capture packets (or headers)
- Not intrusive at all
- Carrier / ISP point of view
- Best solution for a carrier to measure traffic

- Drawbacks
  - Sampling issues
    - IRTF WG → IMRG
  - Difficult to get a user point of view
  - Technical limits (speed of components, capacity)

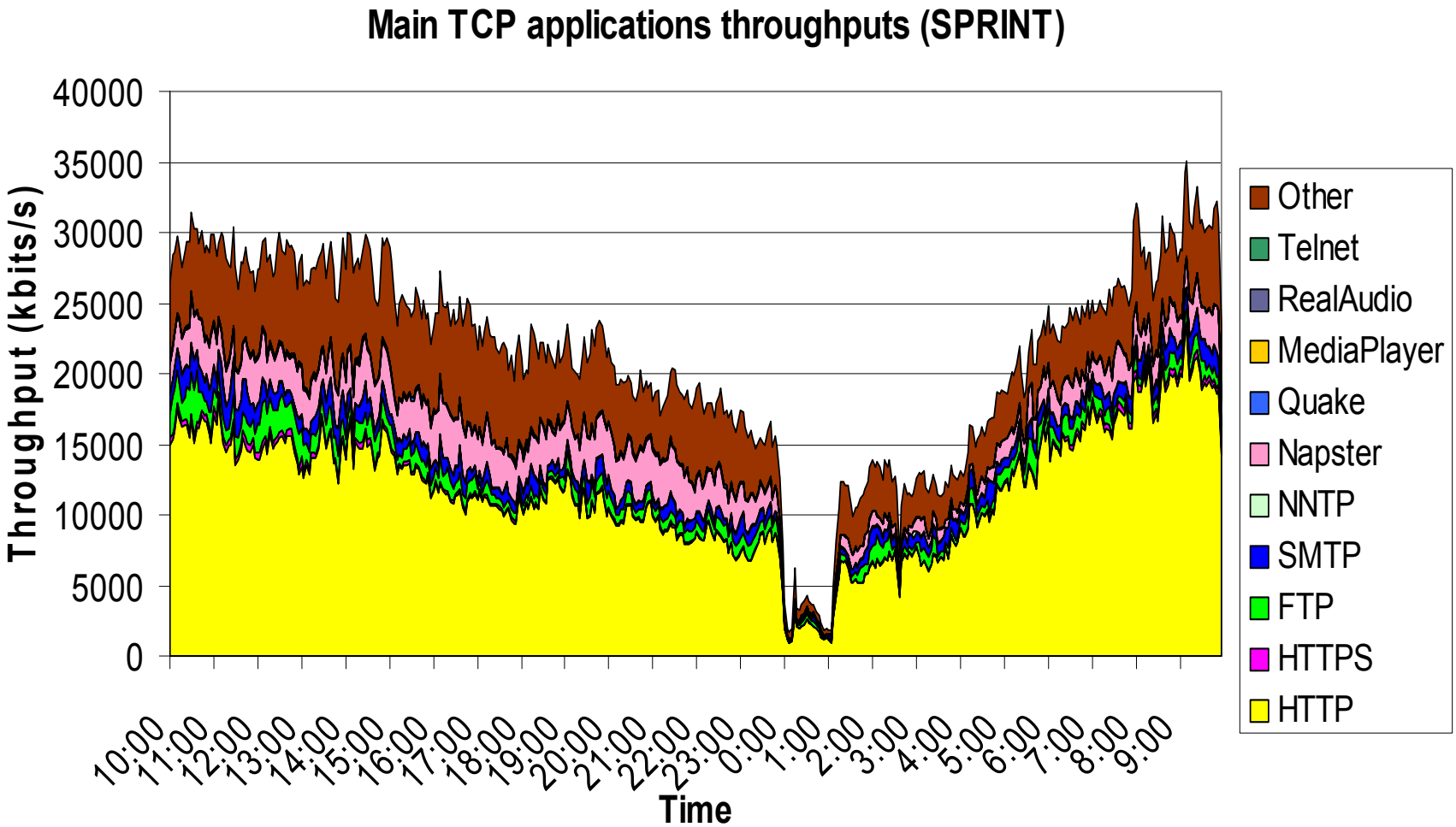
On line vs. Off line measurements

- On line
  - Packets are analyzed in real-time
  - Analysis on very long periods
  - But complexity of analysis is quite limited
- Off line
  - Packets are stored on hard drives / SAN for later analysis
  - Possibilities of analysis are endless
  - Possibility of correlating several traces
  - But amount of stored data is really huge (small periods only)

Internet traffic evolution (May 2000)

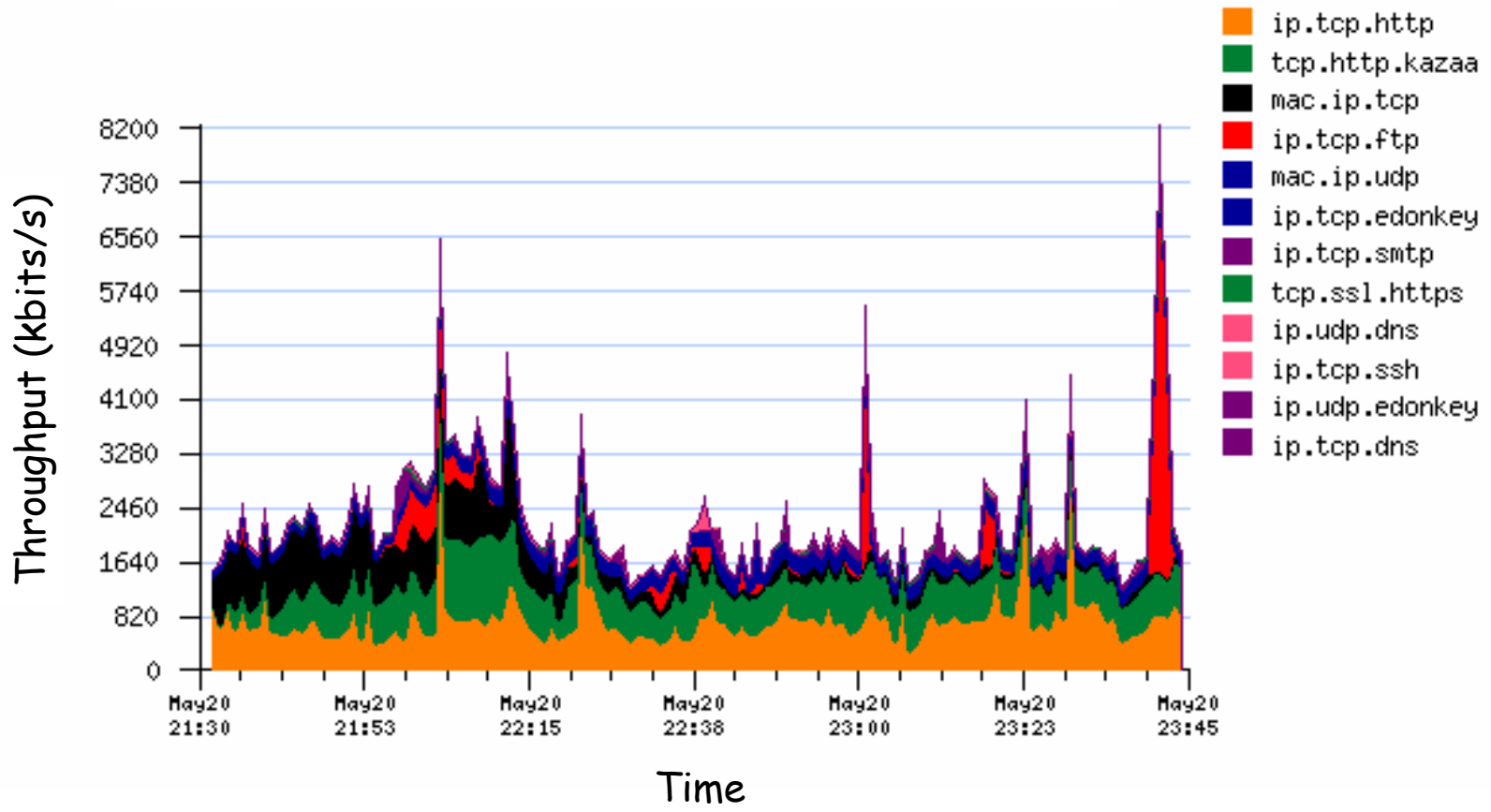


Internet traffic evolution (August 2000)



Internet traffic evolution (May 2003)

Main TCP applications throughputs (Renater)

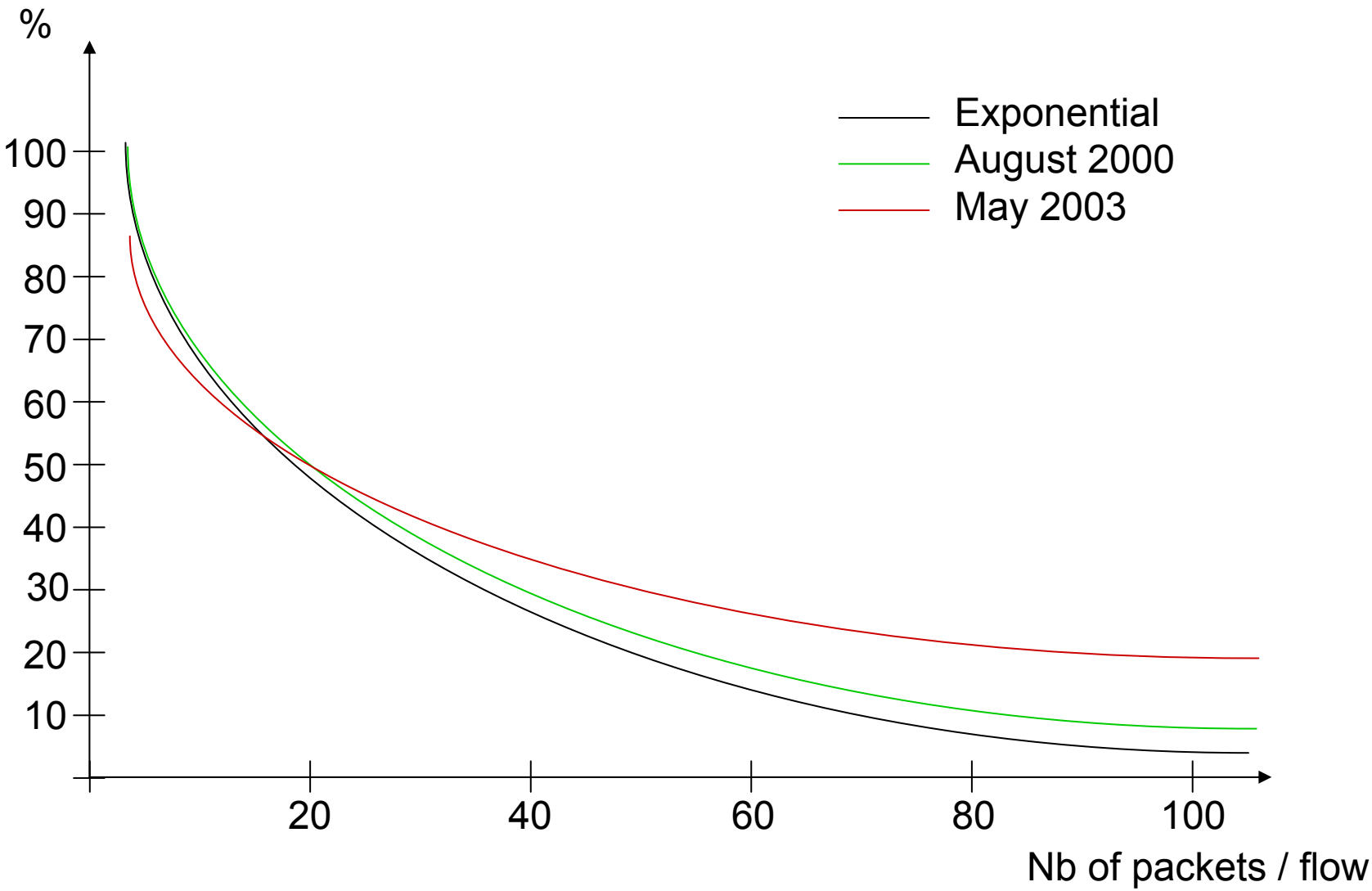


Impact of P2P on traffic

- Thousands of mice
- A large number of elephants

⇨ Change flow size distribution

Flow size distribution



Traffic oscillation issues

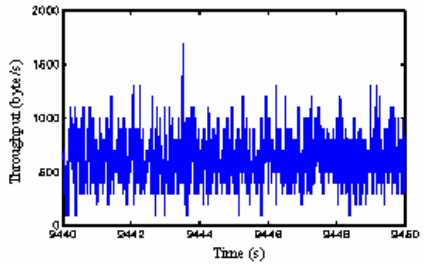
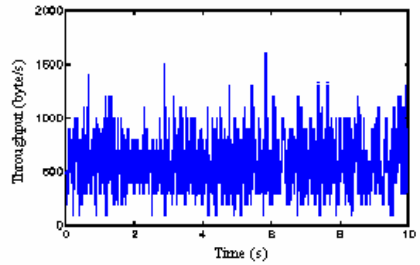
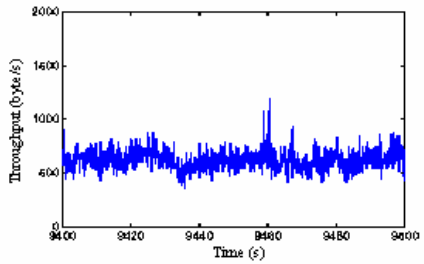
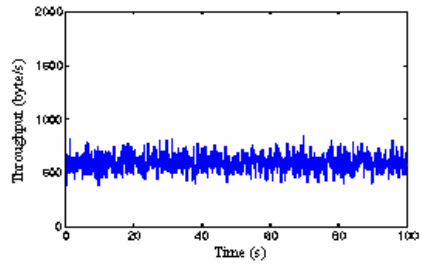
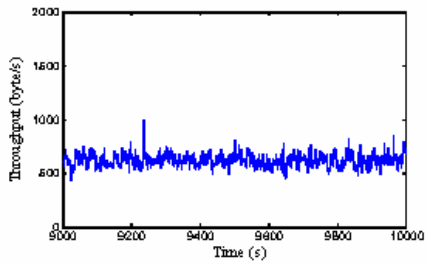
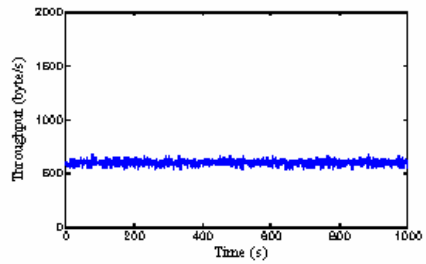
Integrated Throughput on:	IP traffic	Simulated Poisson traffic
0.01 s		
0.1 s		
1 s		

Illustration: LRD and losses

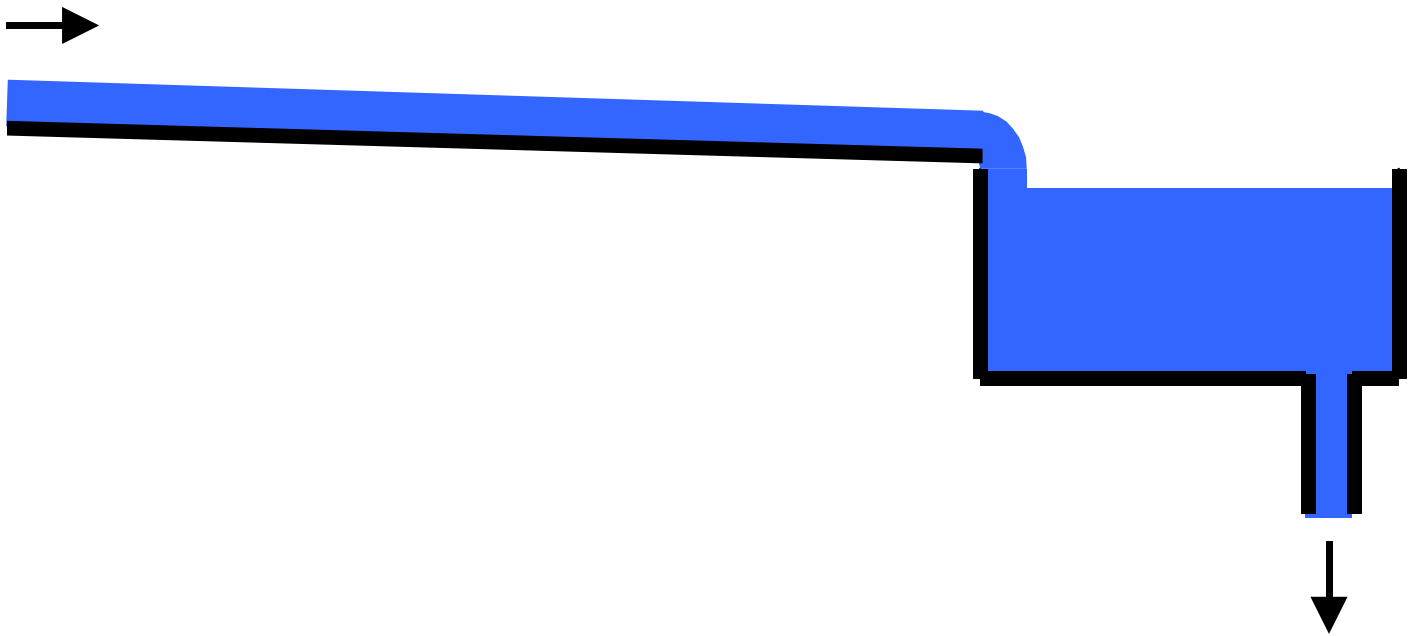


Illustration: LRD and losses

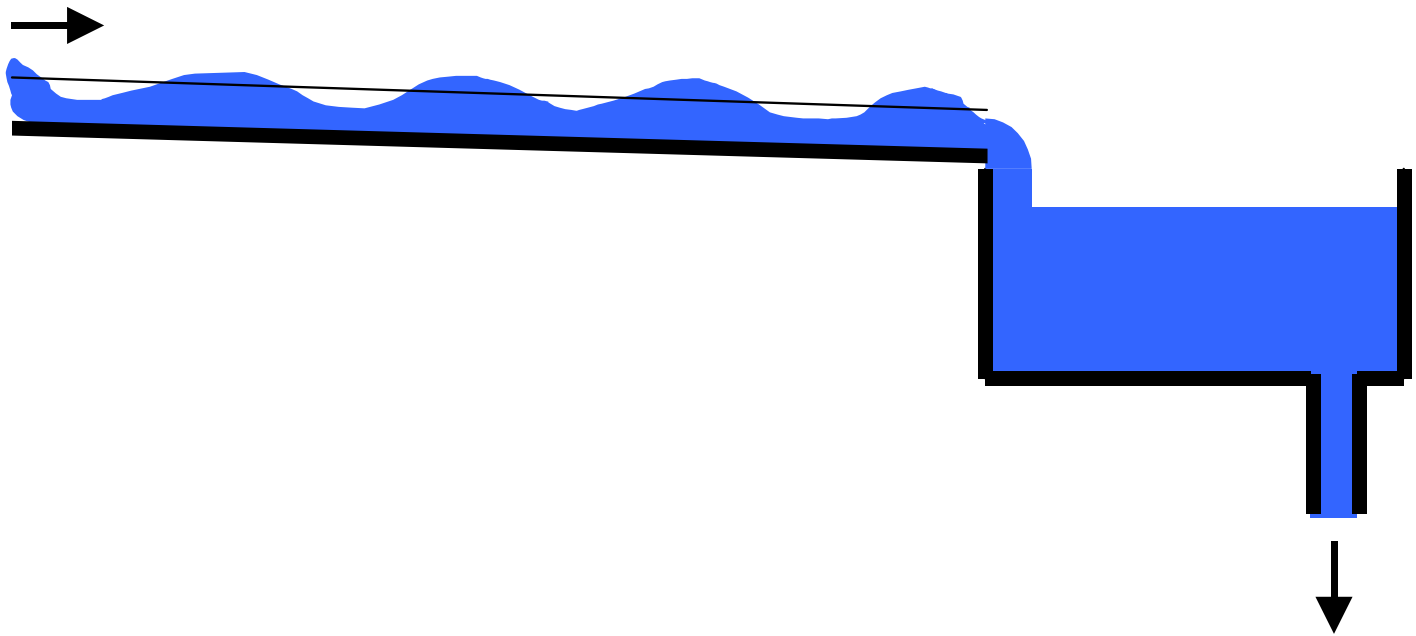


Illustration: LRD and losses

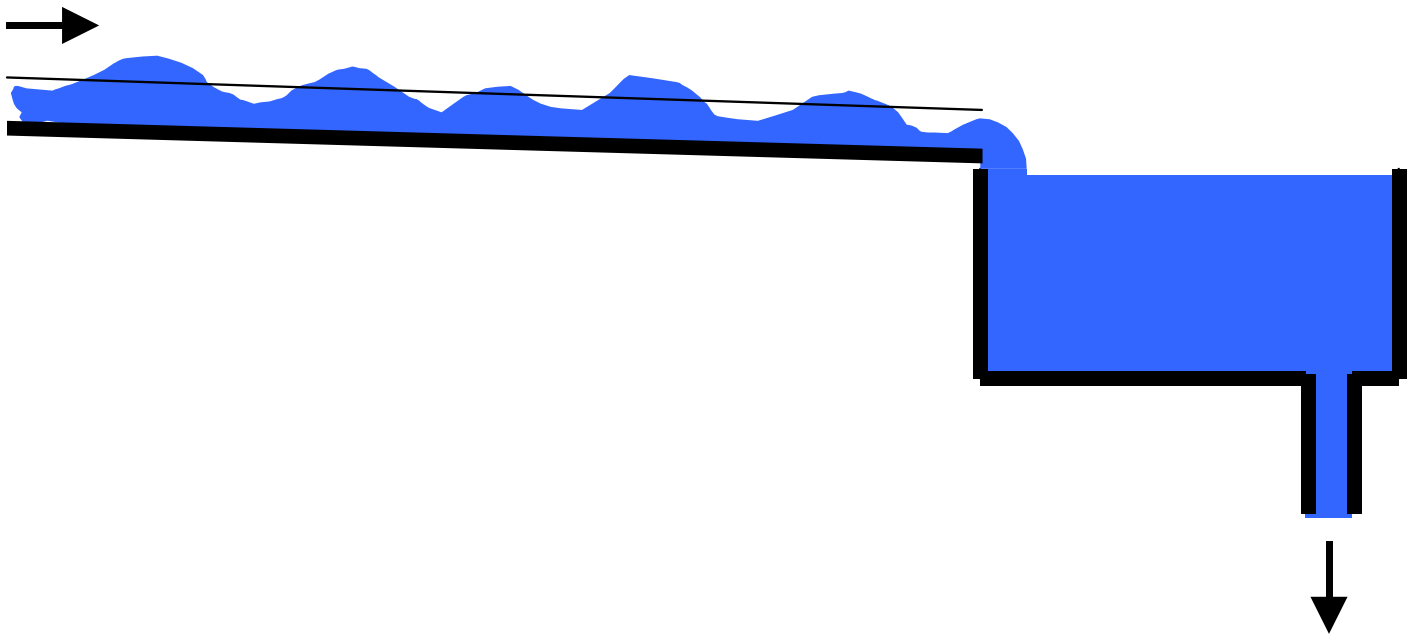


Illustration: LRD and losses

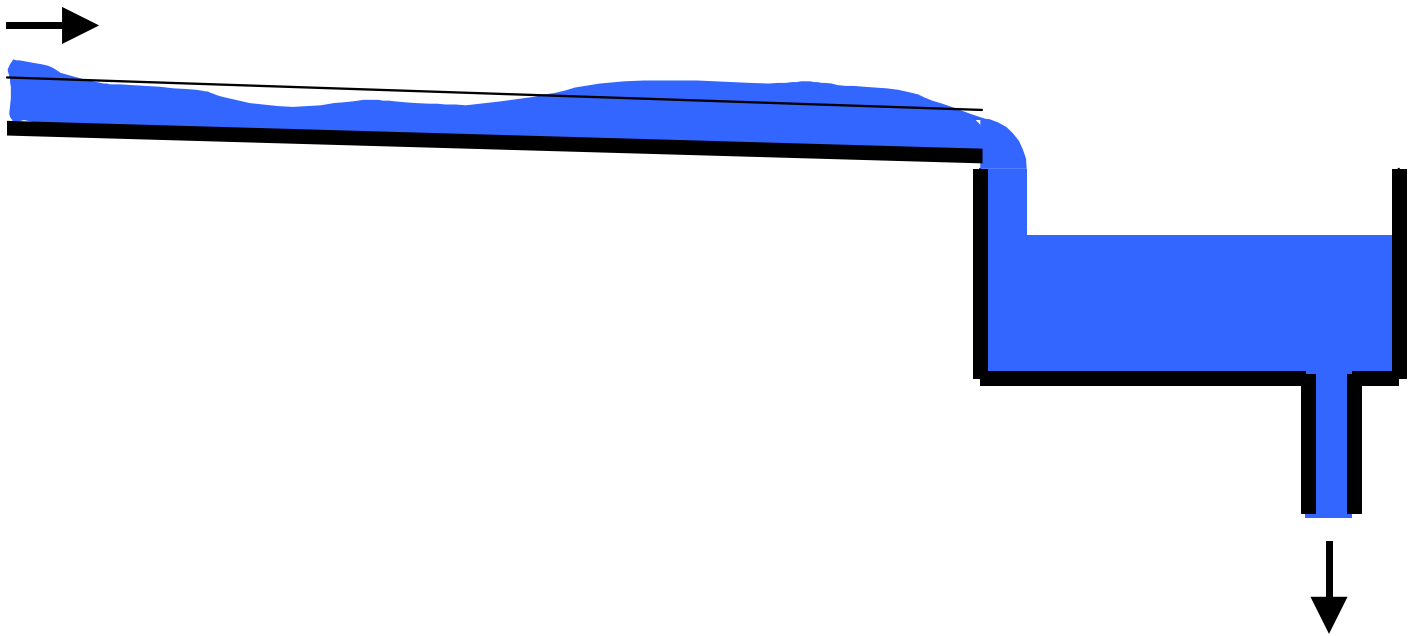
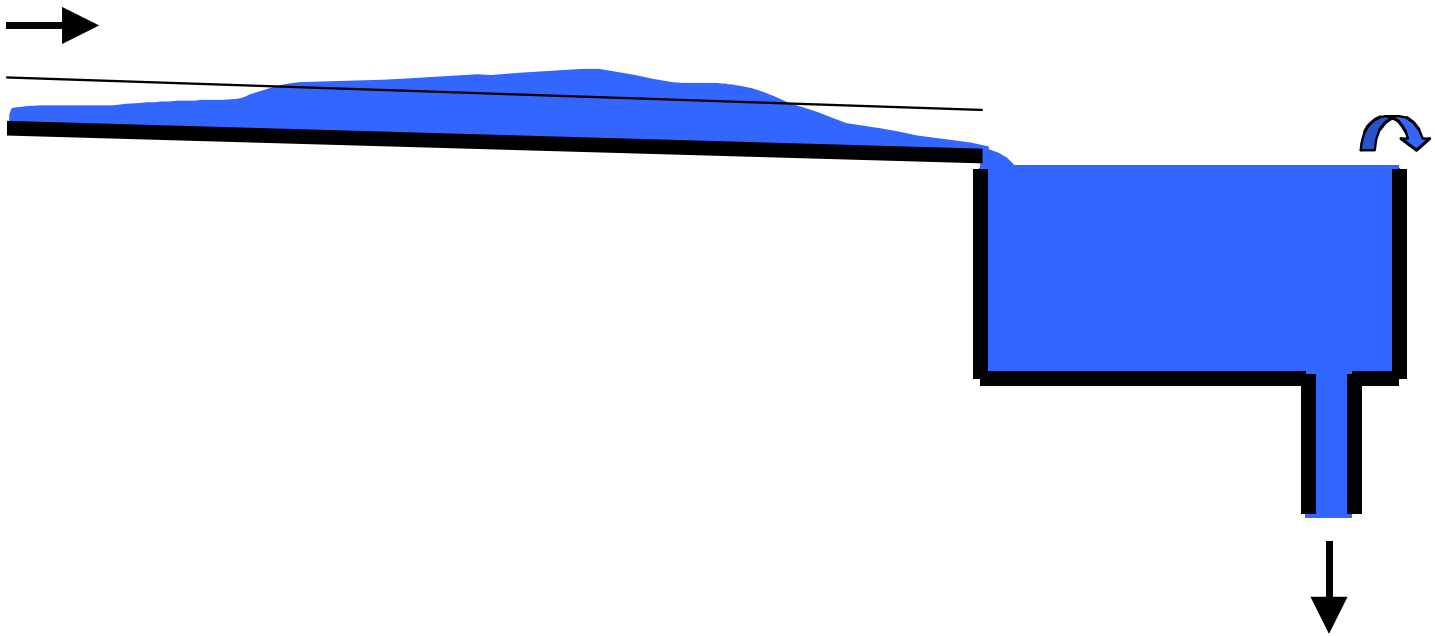
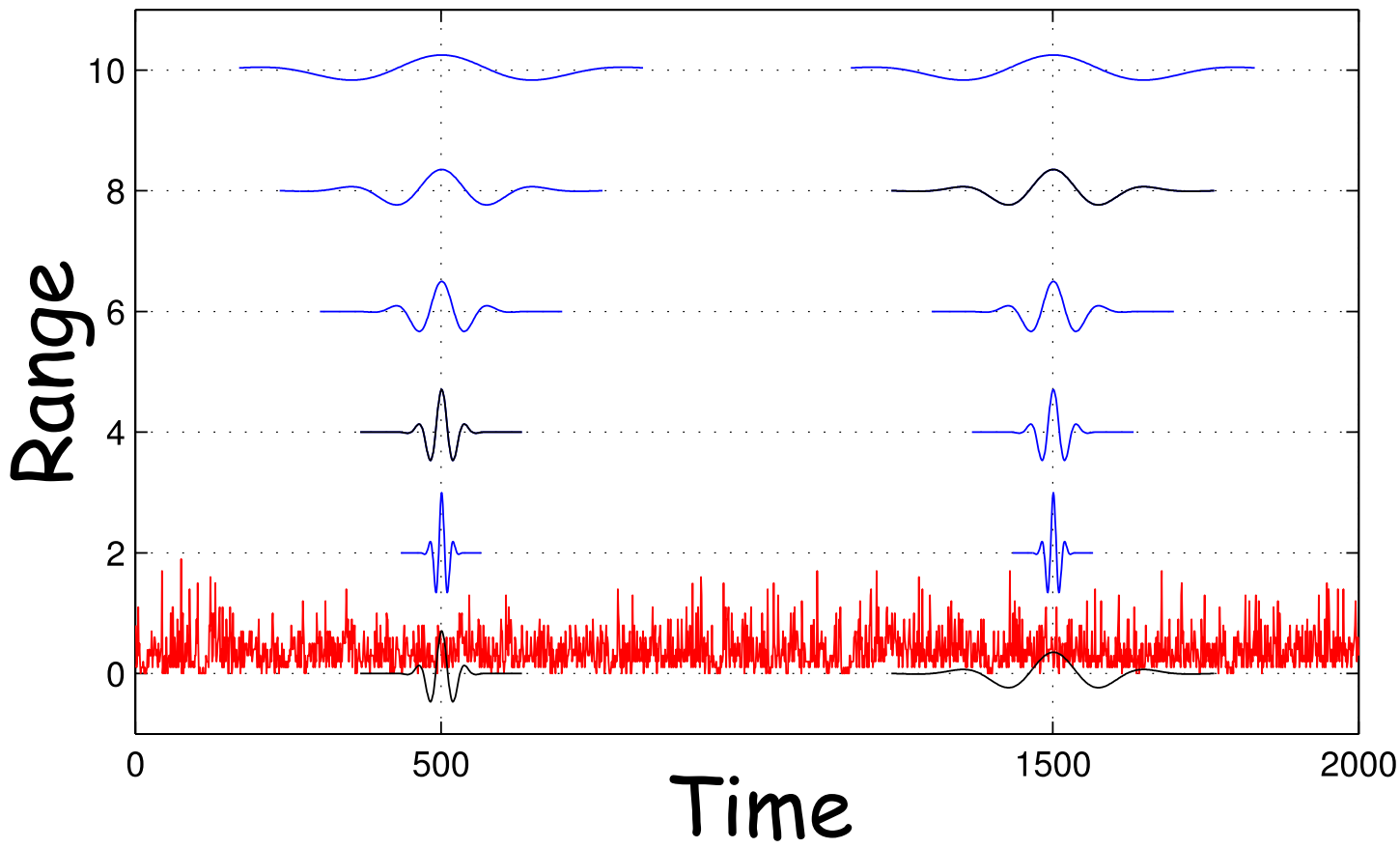


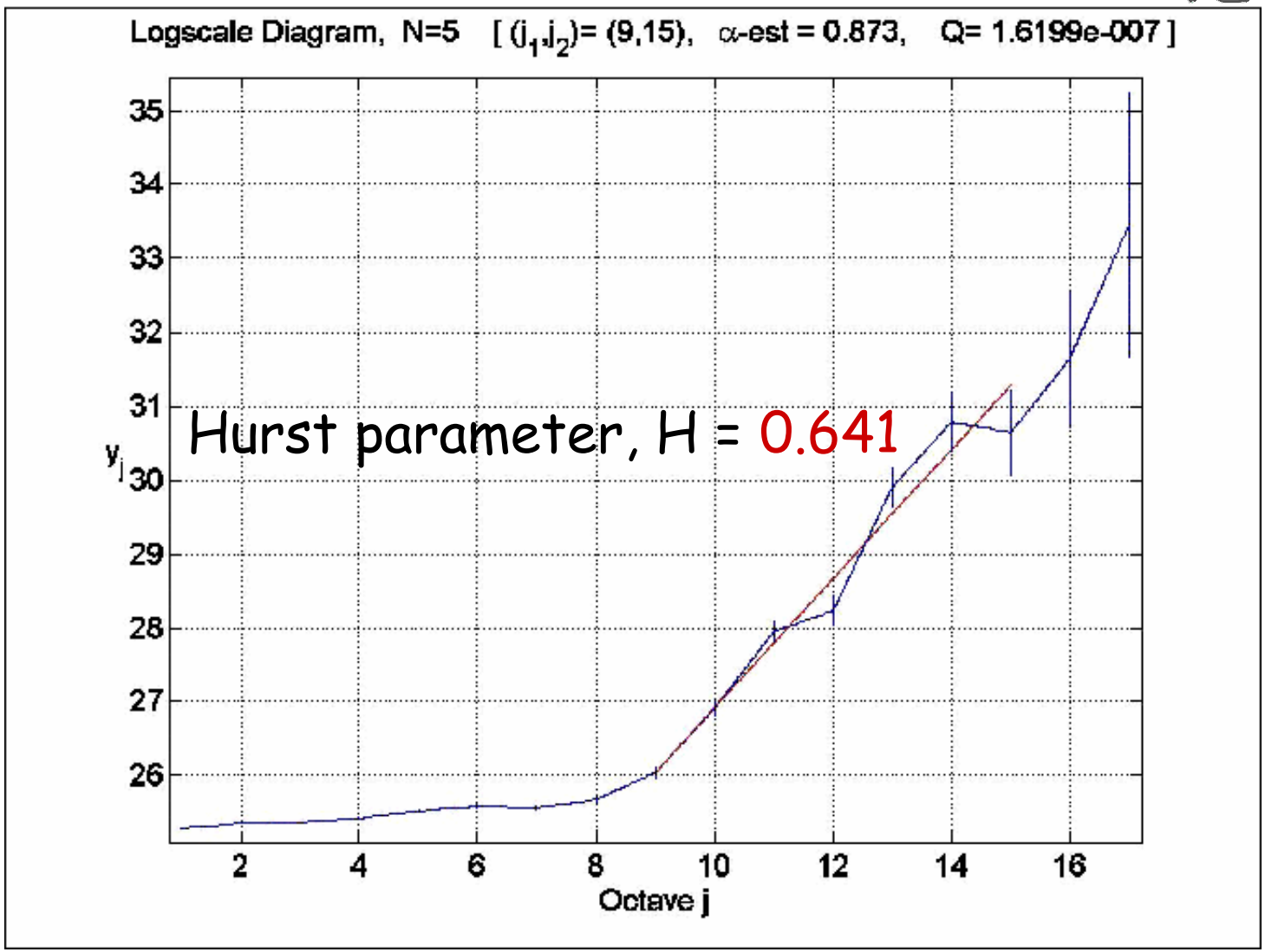
Illustration: LRD and losses



Wavelett analysis of the traffic



Oscillations persistence characterization



Multiple causes for Internet oscillations

1. TCP like congestion control mechanisms
   (Slow Start and Congestion Avoidance mechanisms / Closed control loop)
2. Increase of transmitted file size
3. Increase of network capacities (and over-provisioning)

⇨ Increase of oscillations

- Amplitude
- Range

⇨ traffic oscillations limit network performance
« High variability » paper of Willinger (IEEE ToN 96)

Link between LRD, oscillations and QoS

Disturbances are mainly due to elephants

- What if elephant flows regularity increases?

Principle of the case study

⇨ Use the TFRC mechanism to transmit elephant flows

TFRC principles

- TFRC is a new congestion control mechanism dedicated for stream oriented applications

- TFRC proposes a smooth sending rate with very soft increases and decreases
  - Computed once by RTT by receiver
  - According to the loss event rate (LER)

LER = a loss event is considered if at least one loss appears in a RTT

Experiment description

Objective: comparative evaluation of the global traffic characteristics if elephants use TCP or TFRC as the transmission protocol

Start points:

- Traffic profile based on microscopic monitoring traces
- NS-2 simulations based on replaying actual traffic traces

Simulation principles:

- Elephant flows are transmitted using TFRC
- Others flows use TCP New Reno

Traffic parameters

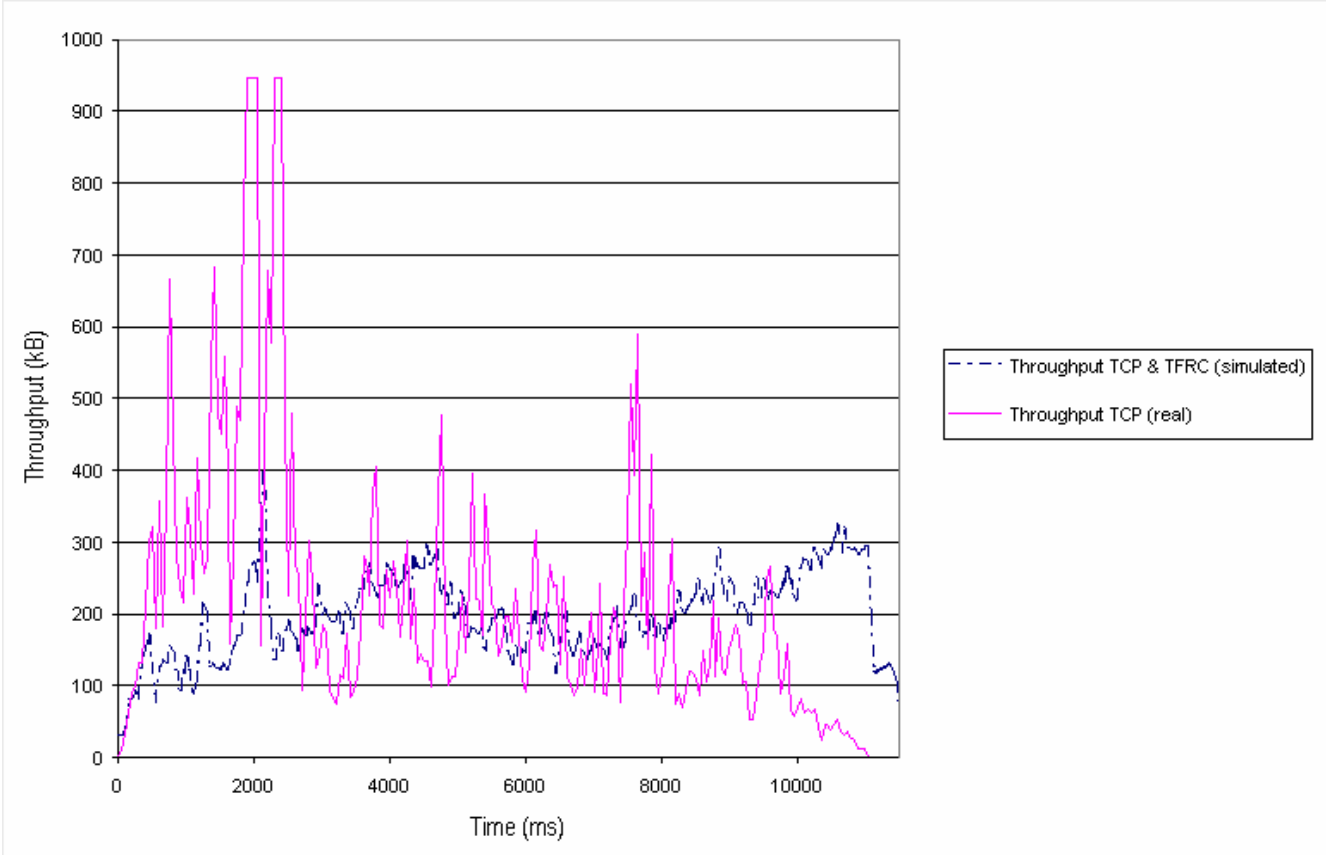
- Classical traffic ones: throughput mean and standard deviation

- One related to traffic variability:

$$\text{Stability Coefficient } (SC) = \frac{\text{exchanged average traffic}}{\text{exchanged traffic standard deviation } (\sigma)}$$

- QoS statistical one: LRD (Hurst parameter)
  - ⇨ Estimation of traffic oscillating range

TFRC impact on flow QoS: throughput analysis

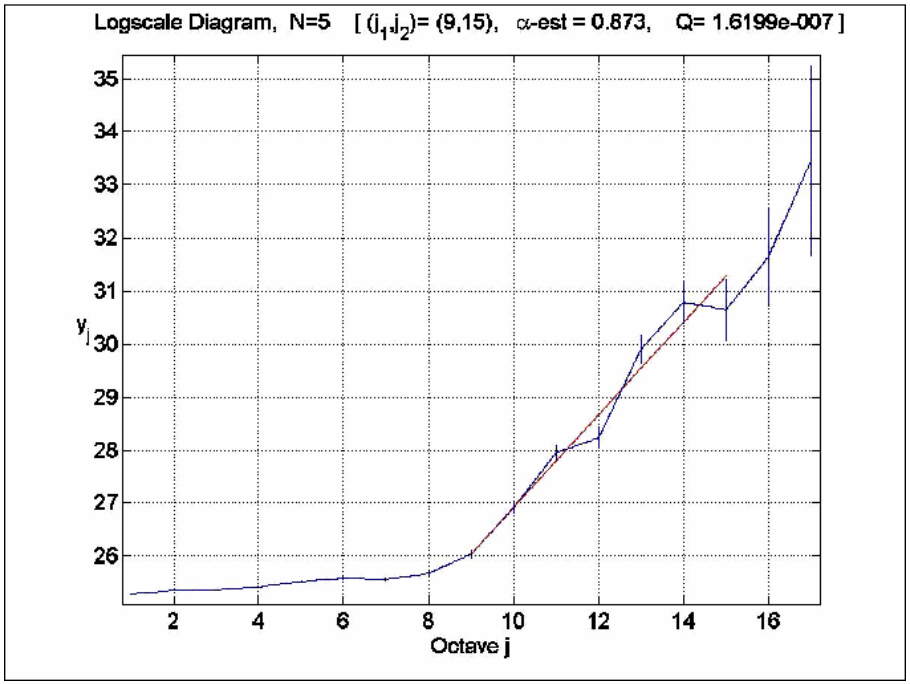


Protocol	Average troughput (kB)	Throughput σ (kB)	SC
TCP New Reno (NR): real case	82.335	157.959	0.521
TCP NR & TFRC: simulated case	77.707	102.176	0.761

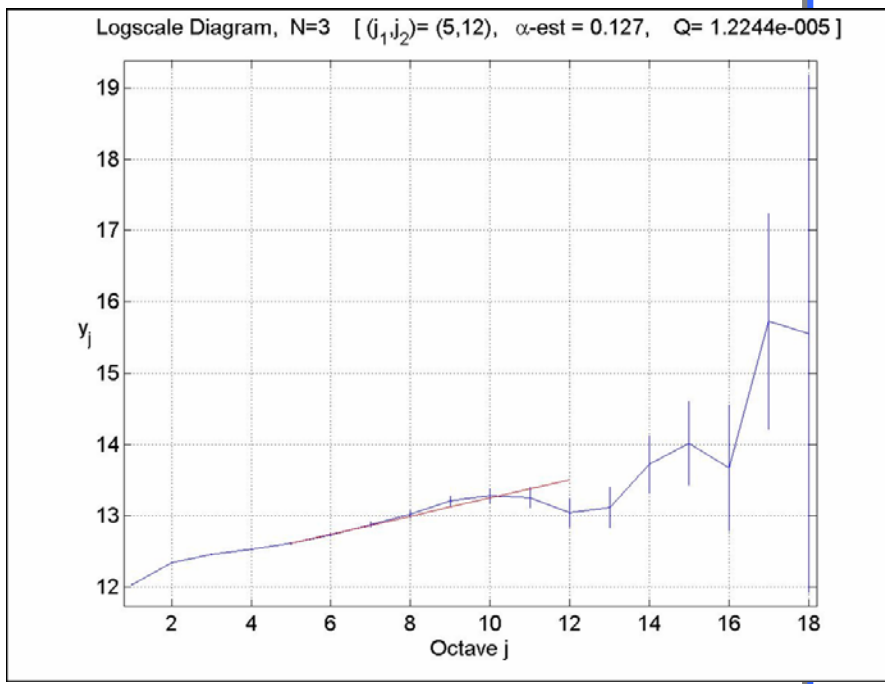
Table 1. Throughput evolution during time for TCP and TFRC protocols

TFRC impact on flow QoS: LRD analysis

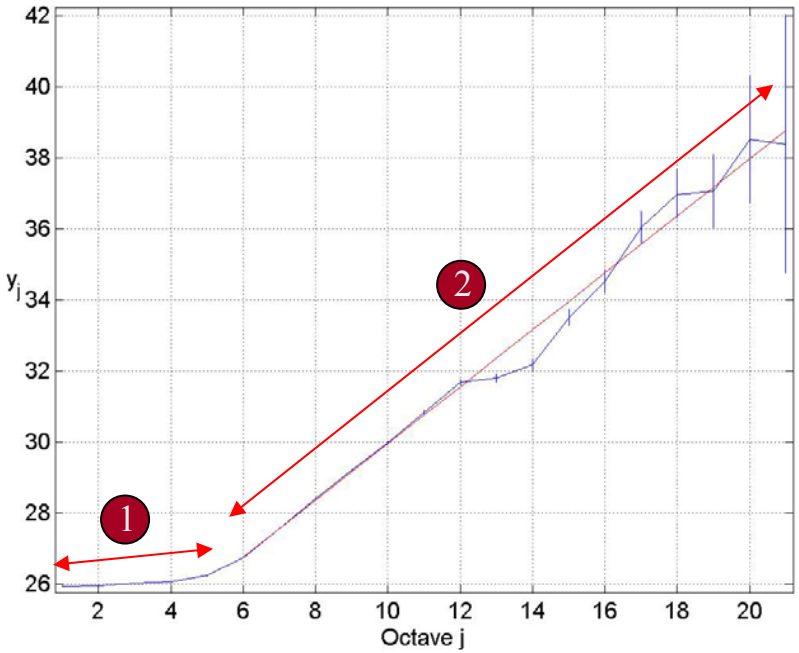
Real traffic

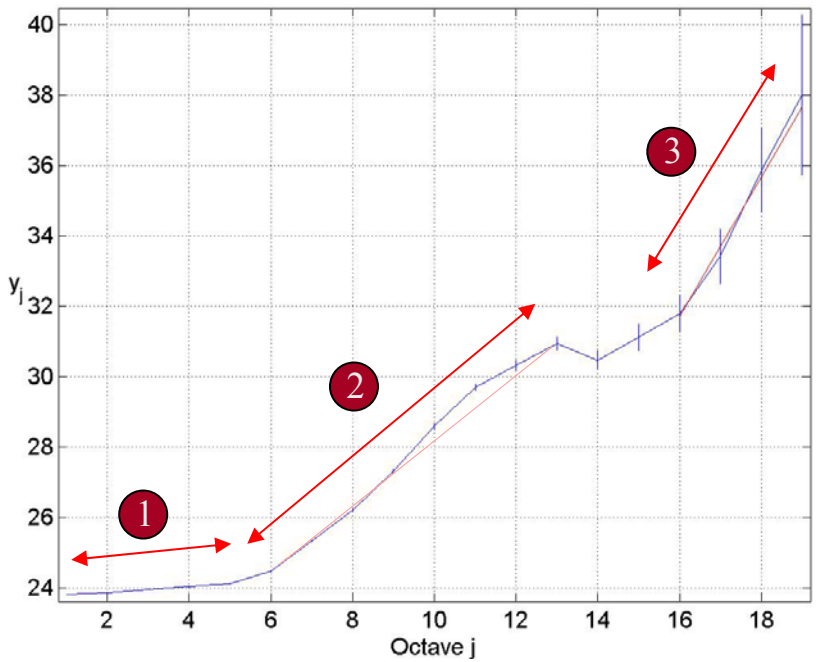


Simulated traffic



LRD due to a UDP flooding attack





Partial conclusion

1. Traffic oscillations highlighted:
   - Causes (TCP + elephants + network capacity)
   - Illustration of the bad impact of LRD on QoS
2. TFRC which generates smoother traffic than TCP
   - Helps to optimize performances
   - Smoothing traffic is essential for being able to guarantee stable QoS
   - Validate the use of LRD to characterize oscillations

But…

- TFRC limitation problem: it cannot generate more traffic than TCP (equation based…)

➔it cannot benefit from the traffic characteristics improvements

Additional problematics (1)

New traffic analysis exhibited that:

- Traffic characteristics are different on different links, at different times…
- Traffic is not stationary
- Many ruptures arises
  - On daily, weekly, monthly yearly basis
  - Random unexpected ruptures
    - Failures, Byzanthin behaviours
    - DoS attacks
    - Legitimate traffic

Additional problematics (2)

Topological issues for end to end QoS

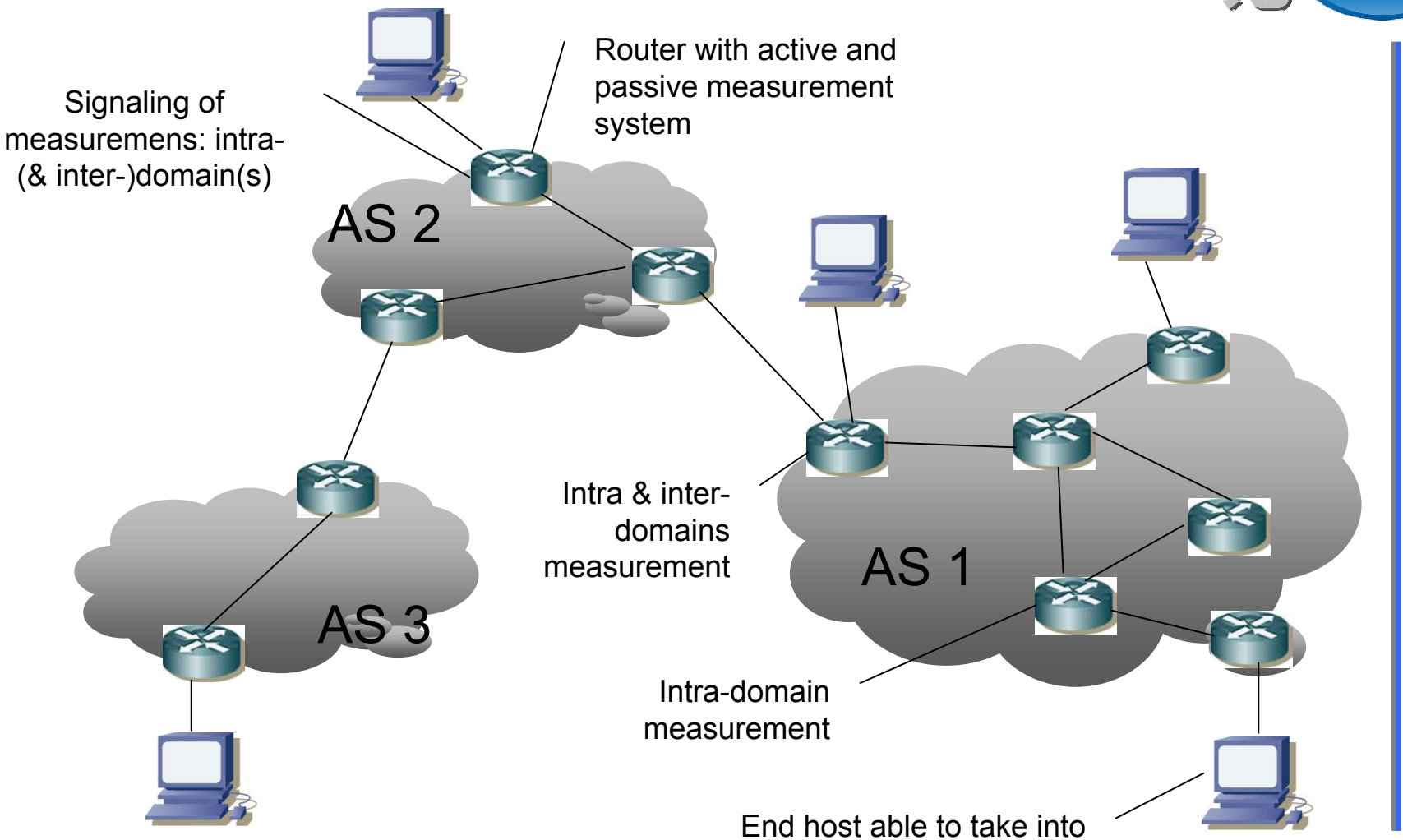
- The Internet is split into AS and domains
- Each domain / AS is designed and managed without regard of other domains / AS
- Few cooperations between carriers and ISP → they are competing to attract clients

Measurement Based Networking

Principle : Extend preceding approach (MBNE) with mechanisms reacting in real time to measurements performed in a large number of points of the network

- Points to address :
  - RT measurement system (passive and active)
  - Measurements signaling
  - Mechanisms to reacting to measurements (routers or end hosts)

Measurement Based Architecture



RT measurement system

- What to measure ?
  - Throughput (passive in intra-domain, active in inter-domains) and available capacities
  - Ruptures in the traffic (attacks, events driven, …)
  - Traffic matrices
  - Oscillations
  - Losses
  - Delays
  - …
- RT → what granularity?

Signaling system and protocol

- What parameter to signal ?
- How to signal these parameters ?
  - COPS, SIP, BGRP, …
  - Mcast/P2P/… ?, Push/pull ?

Reaction to measurements

- How to react to measurements ?
- Are measurements trustable?
  - Especially for inter-domain on a market where comptetition is the standard
- What to do if measurements are missing?
  - Signaling issue if the network is congested

→ Differentiated QoS services (PQ, …)

→Game theory : dead reckoning

Conclusion

- MBNE (Network Engineering) → MBN
- MBN/MBA proved to work well

- Promising approach in many areas
  - QoS
  - Security
  - Management
  - routing
  - Etc.

… But still a lot of work to do