IP Network Monitoring and Measurements: Techniques and Experiences

Philippe Owezarski

LAAS-CNRS
Toulouse, France
Owe@laas.fr

Outline

- Introduction
- Monitoring problematic
  - Only based on network administration tools
  - Problematic example
- Description of monitoring / measurement systems and projects
- Traffic characterization and modeling

Introduction

- Deals with both monitoring results and effects on network design, research and management
- Framework of METROPOLIS
- Topic under the spotlight

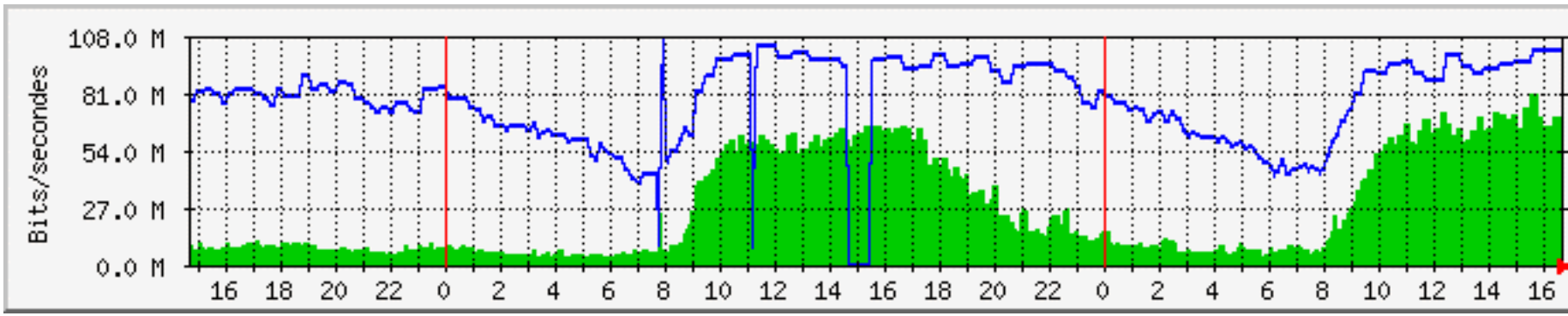
Common solutions for network monitoring

What to use for network monitoring?

- Administration / operation tools based on SNMP
  - Topology of networks / configuration
  - Some statistics measurements
    - Granularity is too coarse: min = 5 s (but can be 1 hour, 1 day, 1 week or whatever)
    - Measured parameters are more or less the amount of traffic sent and received

Some examples of SNMP results

RAP ↔ RENATER interconnection

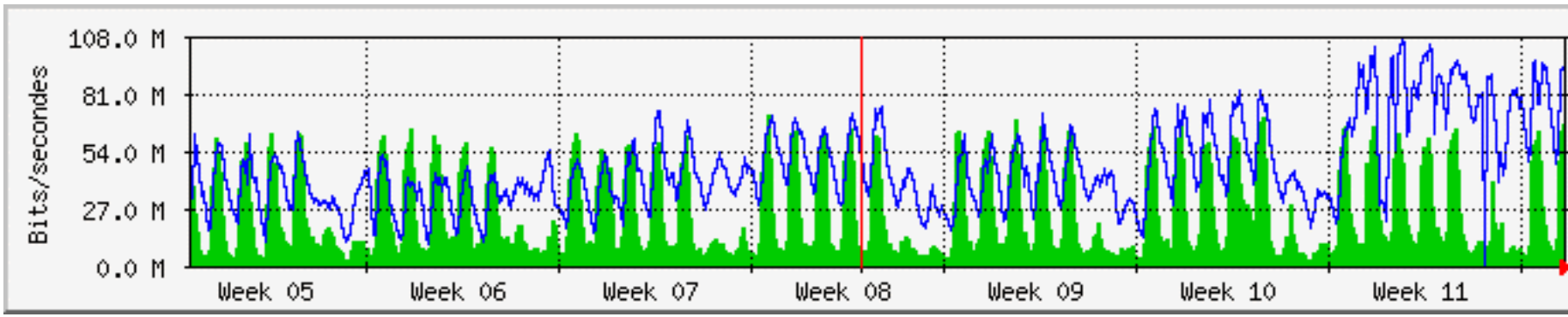


Per hour trace

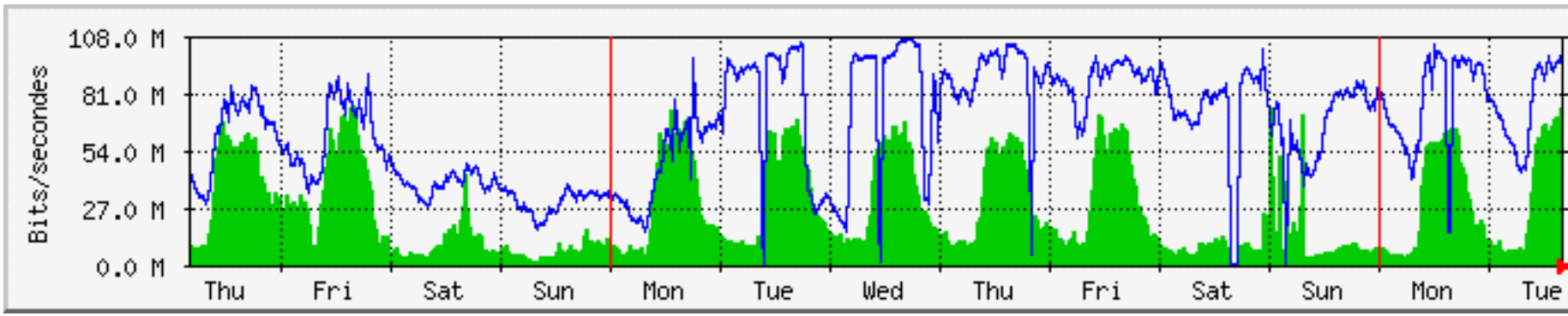
Input traffic

Output traffic

Some examples of SNMP results (2)



Per Month trace



Per Week trace

Input traffic

Output traffic

Problems for monitoring networks

- Impossible to monitor traffic dynamics (second order values as variability auto-covariance for instance)
- Impossible to monitor traffic QoS (user point of view – goodput)
- Impossible to get a (formal) traffic model

Example on network provisioning

- Common beliefs tell us traffic is Poisson:
  - $E[X]=\lambda$
  - $V[X]=\lambda$
  - Provisioning should be 2λ
- Actually, provisioning has to be at least 1:3 (i.e. 3λ)
  - RENATER 1:3
  - Sprint 1:3
  - WorldCom 1:5
  - AT&T 1:10

Questions on the example

- How explaining this over-provisioning requirement ?
- How to predict the traffic that will be supported by a new network to design ?

?

IP monitoring: goals and importance

- Network and traffic exist and is full of information
- Help to predict what will be the traffic in the future based on some current trends
- Help to design and provision a network and Internet protocols

IP monitoring: goals & importance (2)

- ⇒ Monitoring changes the network engineering and research process
- ⇒ Monitoring is a new service that must be provided by vendors, carriers and ISP (technical and commercial adds) and strongly requested by users

Monitoring concerns

- Network design
- Traffic engineering / routing tables
- Network management
- Provisioning
- Pricing / charging
- QoS monitoring
- Assessment and tuning of mechanisms as
  - QoS (IntServ, DiffServ, IPv6, MPLS, …)
  - Traffic engineering (OSPF, MPLS…)

IP Monitoring and Research

- New protocols and architectures for:
  - Traffic characterization and modeling
  - Multi-domains QoS guaranty
  - Service and network utilization optimization
  - Network or VPN or CoS provisioning
  - QoS routing
  - Network security
- Techniques and mechanisms for:
  - pricing

State of the art
(as far as I know)

Active vs. Passive Measurements
Some Monitoring Projects

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

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

Some active measurement tools

- Ping
- Traceroute
- MGEN
- RIPE equipments
- Etc.

⇒ Importance of clock synchronization: most of the time GPS is required

Projects based on active measurements

- Projects
  - Surveyor (NSF): ping and GPS clocks
  - NIMI (Paxson/ACIRI) / RIPE
  - MINC (Multicast INC)/ UINC (Unicast INC)
  - Netsizer (Telcordia ex Bellcore)
  - AMP (NLANR)
- Topics
  - Measuring QoS (Delay, loss, RTT, throughput)
  - Infer internal structure of the network
  - Tomography
  - Detect points of congestion

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
    - Creation of a new 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)

Passive measurement tools

- TSTAT
- NTOP
- LIBCAP
- Tcpdump
- Tcptrace
- QOSMOS
- IPANEMA
- CISCO's Netflow
- OCxMON (mainly ATM)

Projects based on passive measurements

- Projects
  - Netscope (AT&T): Based on Netflow
  - CAIDA: Based on OCxMON & Monitoring of vBNS
  - SPRINT IPMON
- Topics
  - Traffic matrices / routing table / Tomography
  - Network security
  - Network provisioning
  - Evolution of traffic (new applications)
  - Representing the Internet
  - Traffic modeling and predictions

METROPOLIS
(supported by RNRT)

Partners

- LIP6
- LAAS
- FT R&D
- GET
- INRIA Rocquencourt
- EURECOM
- RENATER

Objectives

- Defining a monitoring methodology
- Combining active and passive measurements
  - Active: IPANEMA, RIPE, QoSMOS
  - Passive: DAG
- A full set of networks
  - VTHD (high speed experimental network)
  - Renater (public operational network)
  - ADSL (private operational network)

Addressed issues

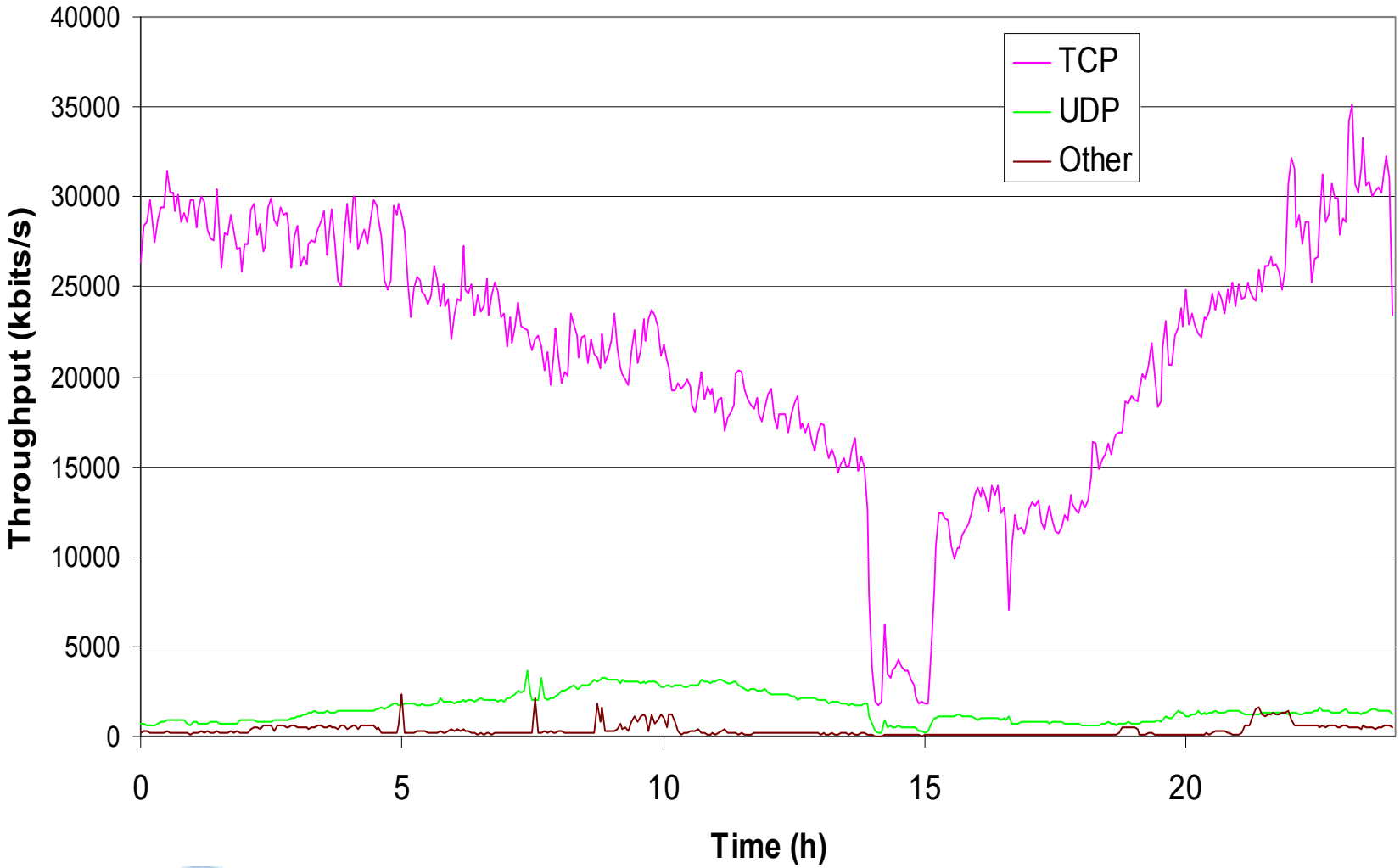
- Empiric and stochastic modeling (and more?)
- Provisioning and SLAs
- Classification
- Traffic, network and protocol analysis
- Sampling
- Pricing and charging

METROPOLIS passive measurements

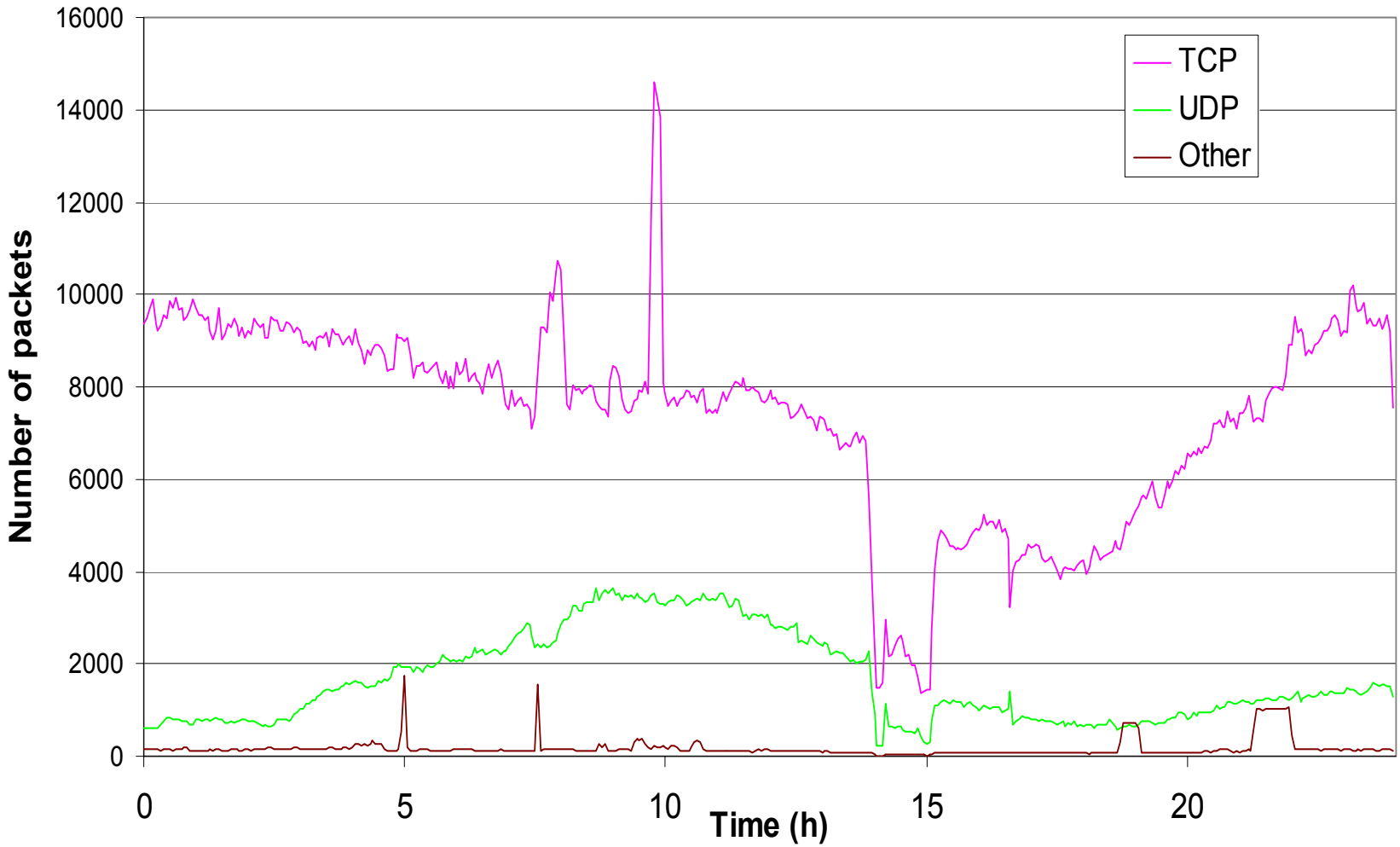
- Insert optical splitter on network links
  → transparent system, not intrusive
- Data from an operational IP backbone
- Integrated system to collect packet-level, flow-level, and routing measurements
  - Collect and timestamp all IP headers (44 bytes) with GPS timestamps (accuracy > 2 μsec)
  - ATM/Ethernet PCI network interface (DAG: University of Waikato /Endace, NZ)

Traffic characterization

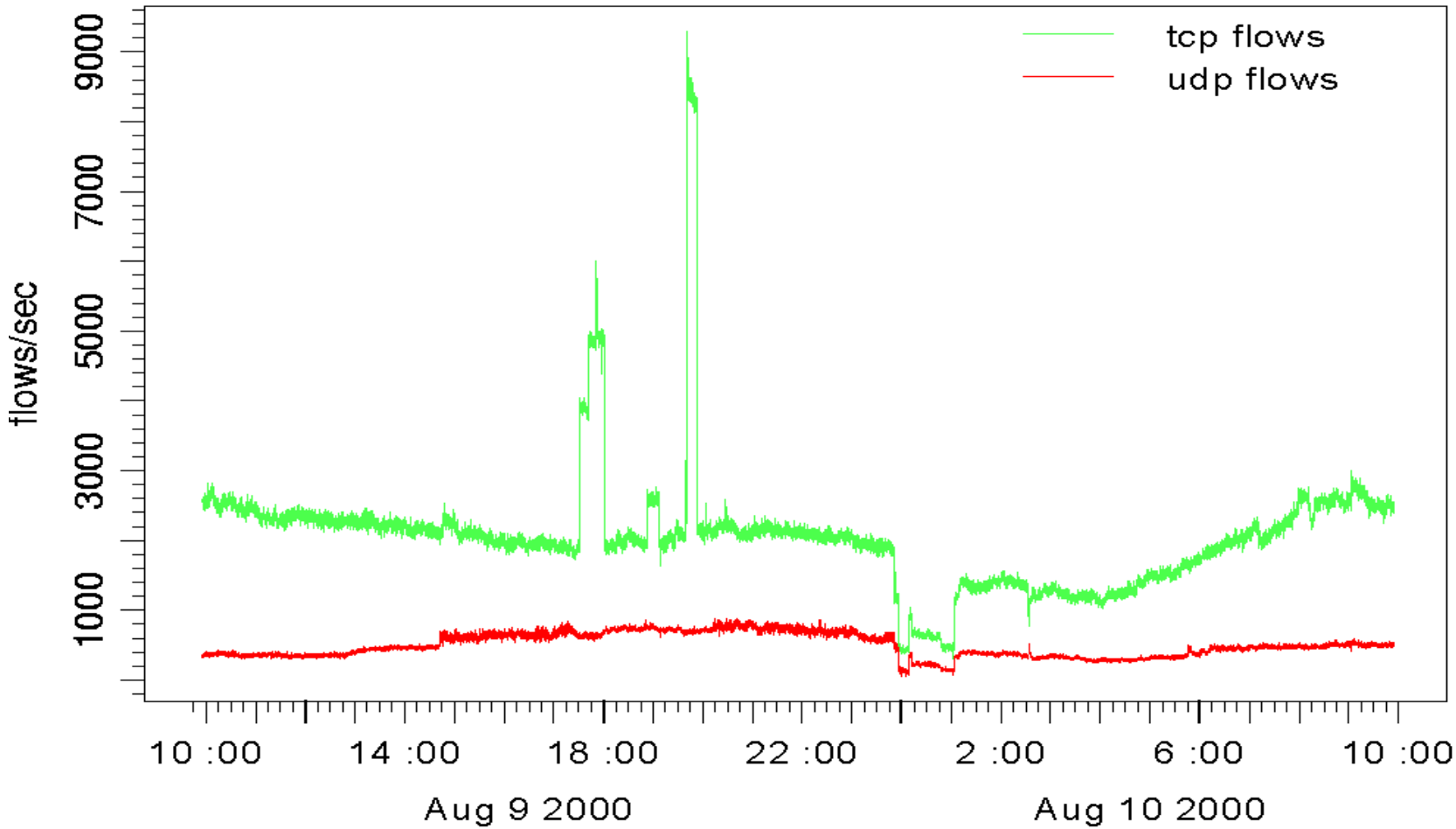
Link Utilization: bandwidth



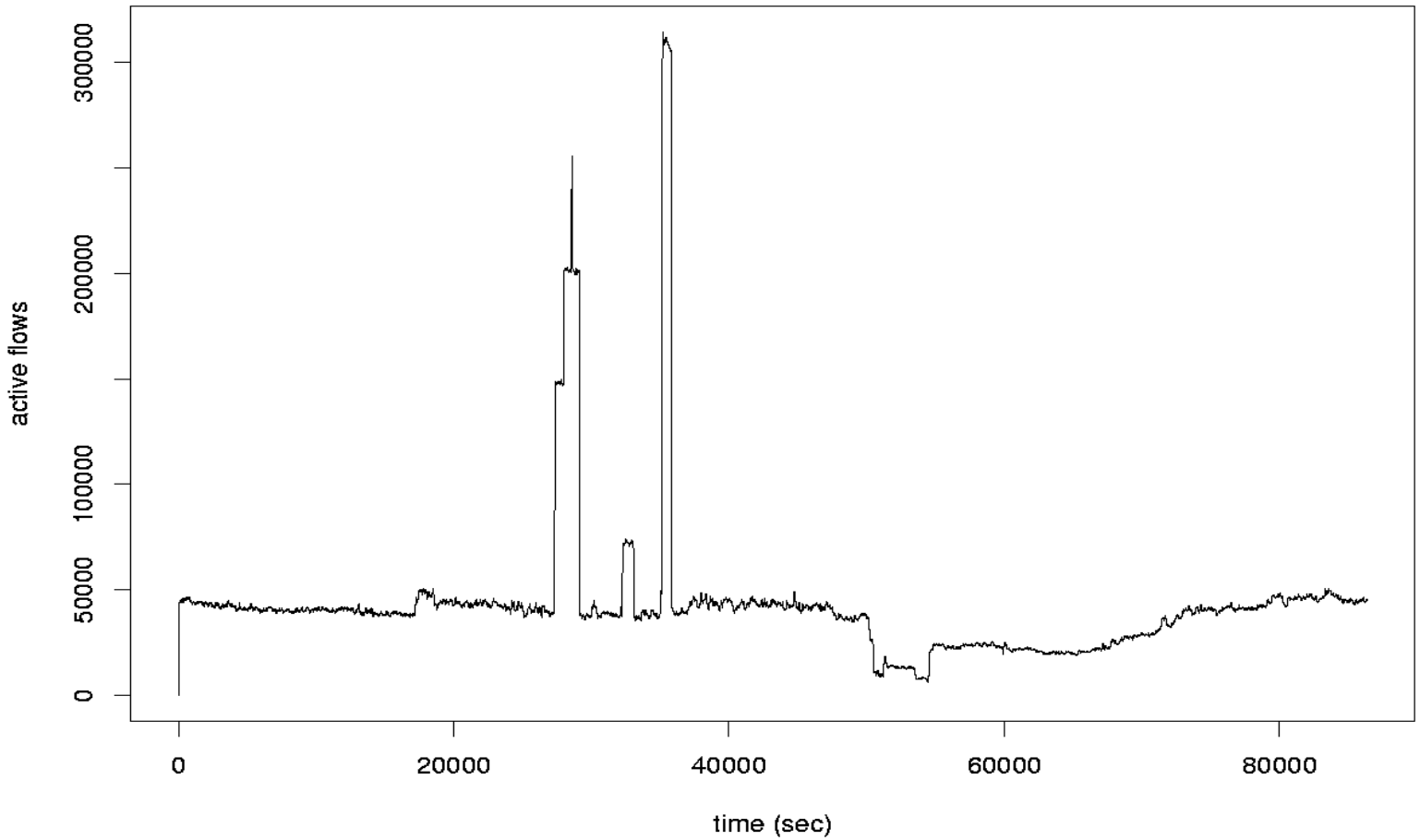
Link utilization: packets



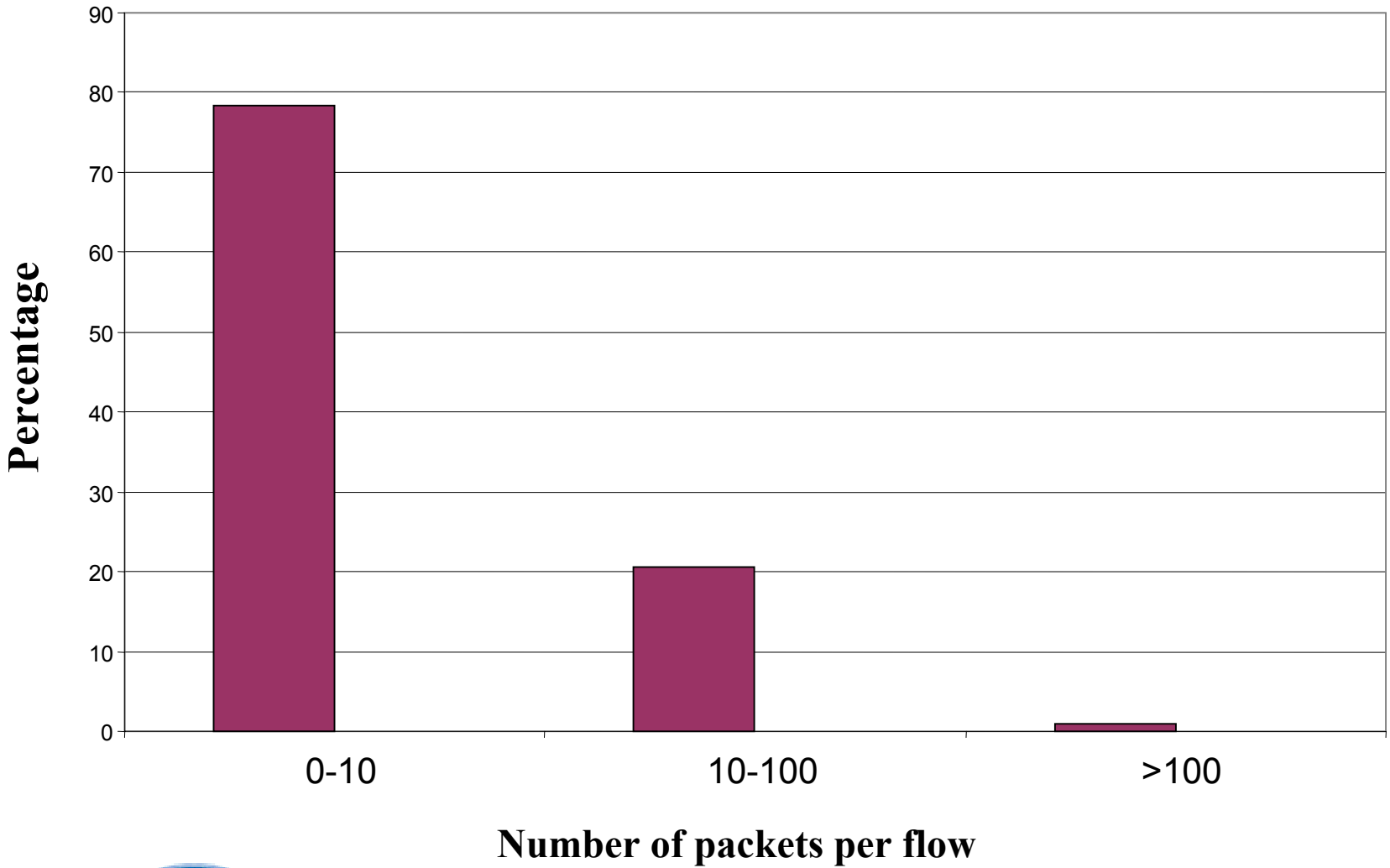
Link utilization: instantaneous flows



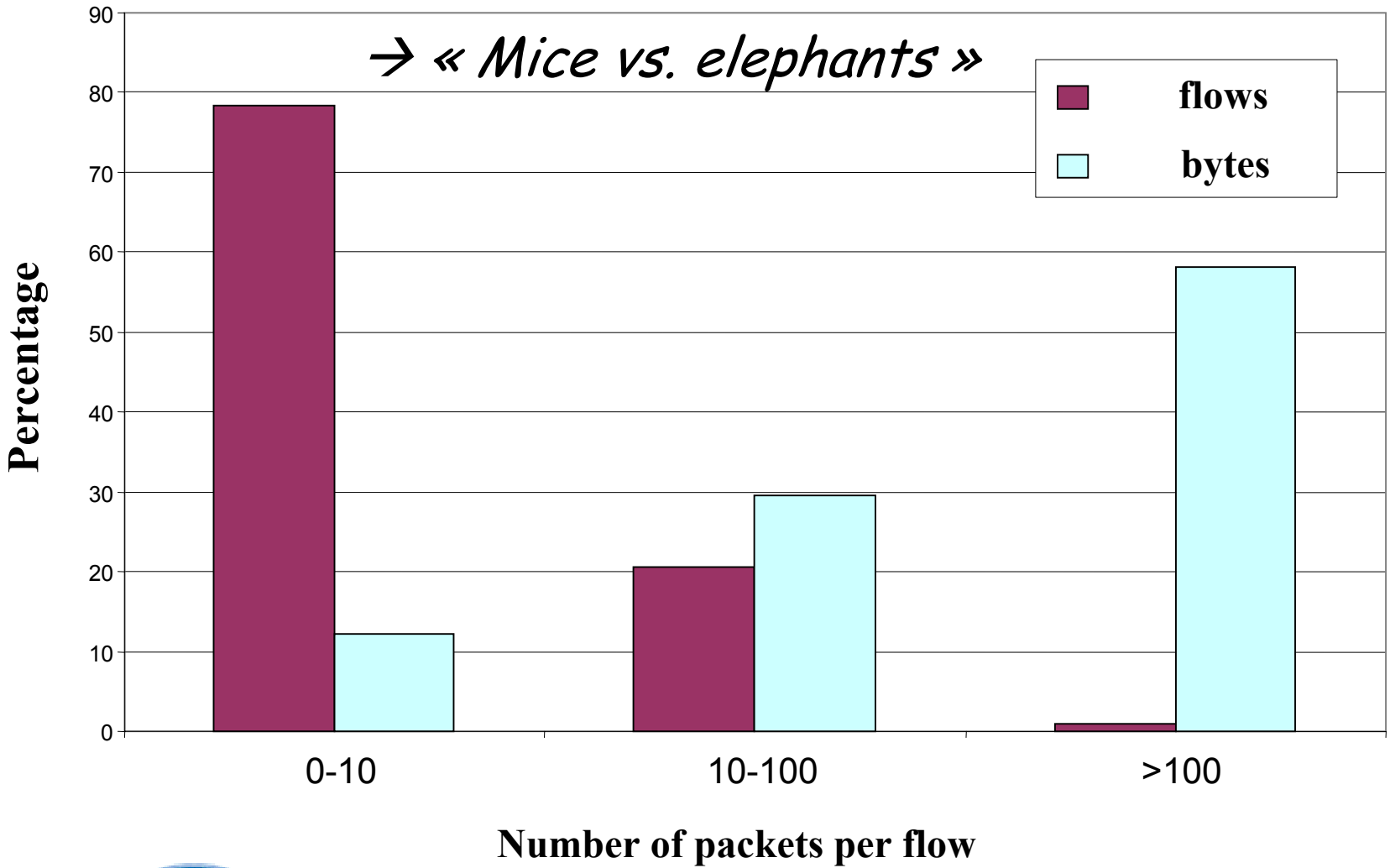
Link utilization: active flows



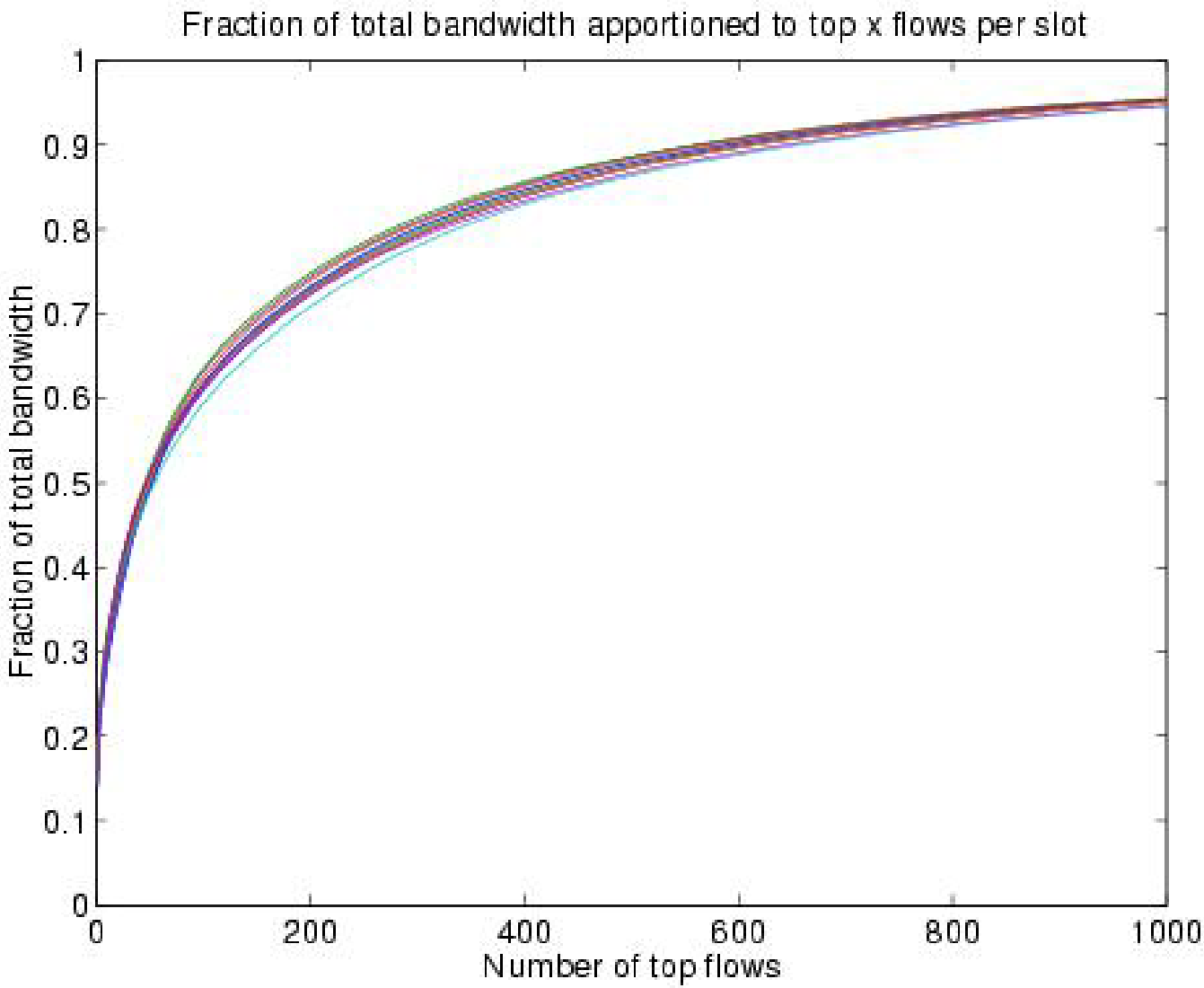
TCP flow size



TCP flow size vs. total bandwidth



Elephants


Fraction of total bandwidth apportioned to top x flows per slot
Fraction of total bandwidth
Number of top flows
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
200
400
600
800
1000

Traffic modeling

Why modeling Internet (TCP) traffic ?

- Different from common thinking i.e. telephone model (Poisson, Gilbert)
- Give information on how designing, managing, ***provisioning*** and operating an IP network
- Give information on future research directions
- Allows researchers to simulate new technical proposals

Previous work on traffic modeling

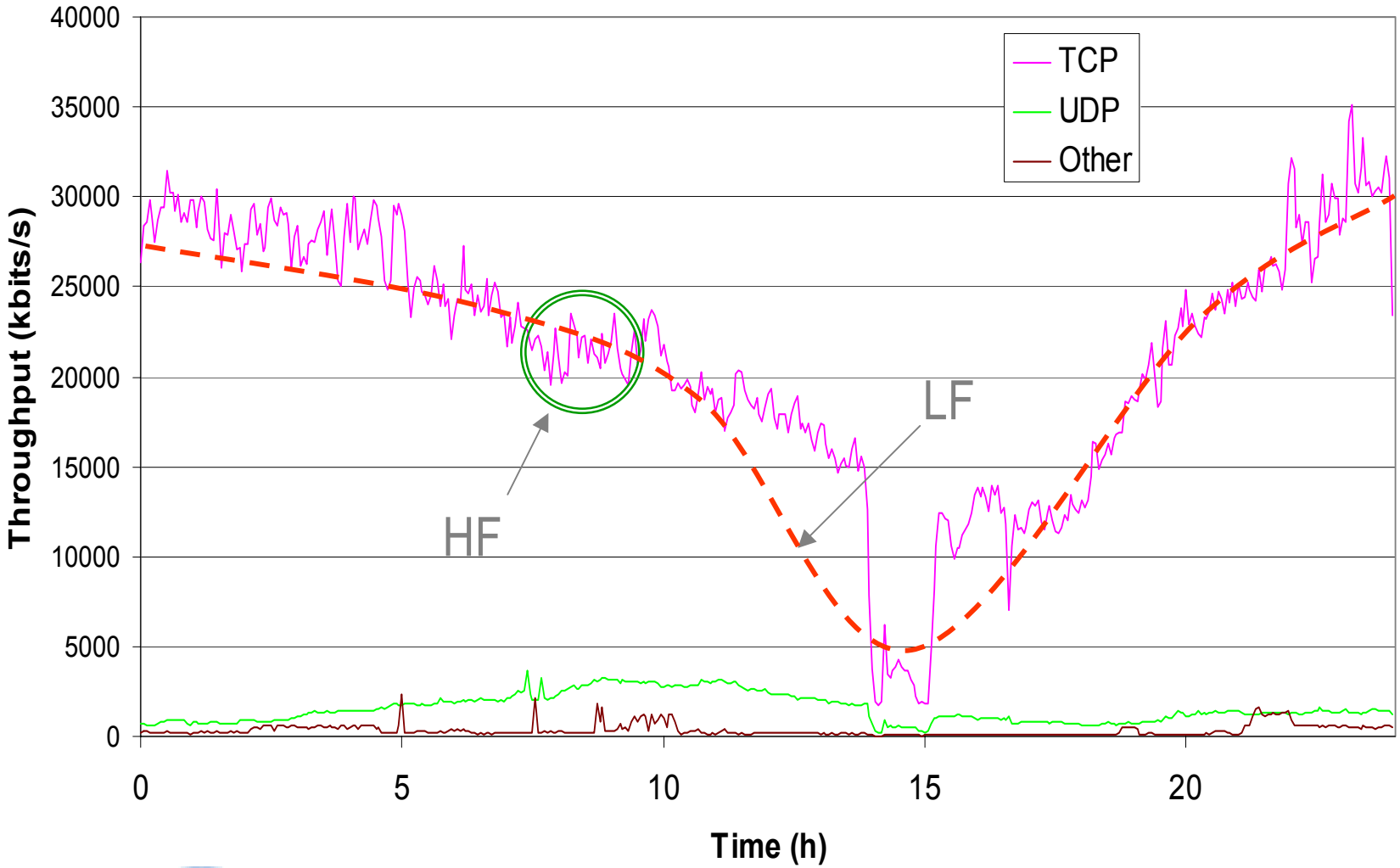
- **Self-similar**
- *Multi-fractal*
- *LRD*

- Due to:
  - Heavy tailed distribution of flow size
  - TCP-like congestion control
  - Routers
  - Human and application behavior

Self-similarity

- Internet traffic is said to be self-similar
- Self-similar ? What does it mean ?
- Is it bad ?

Actual traffic



Actual traffic visual analysis

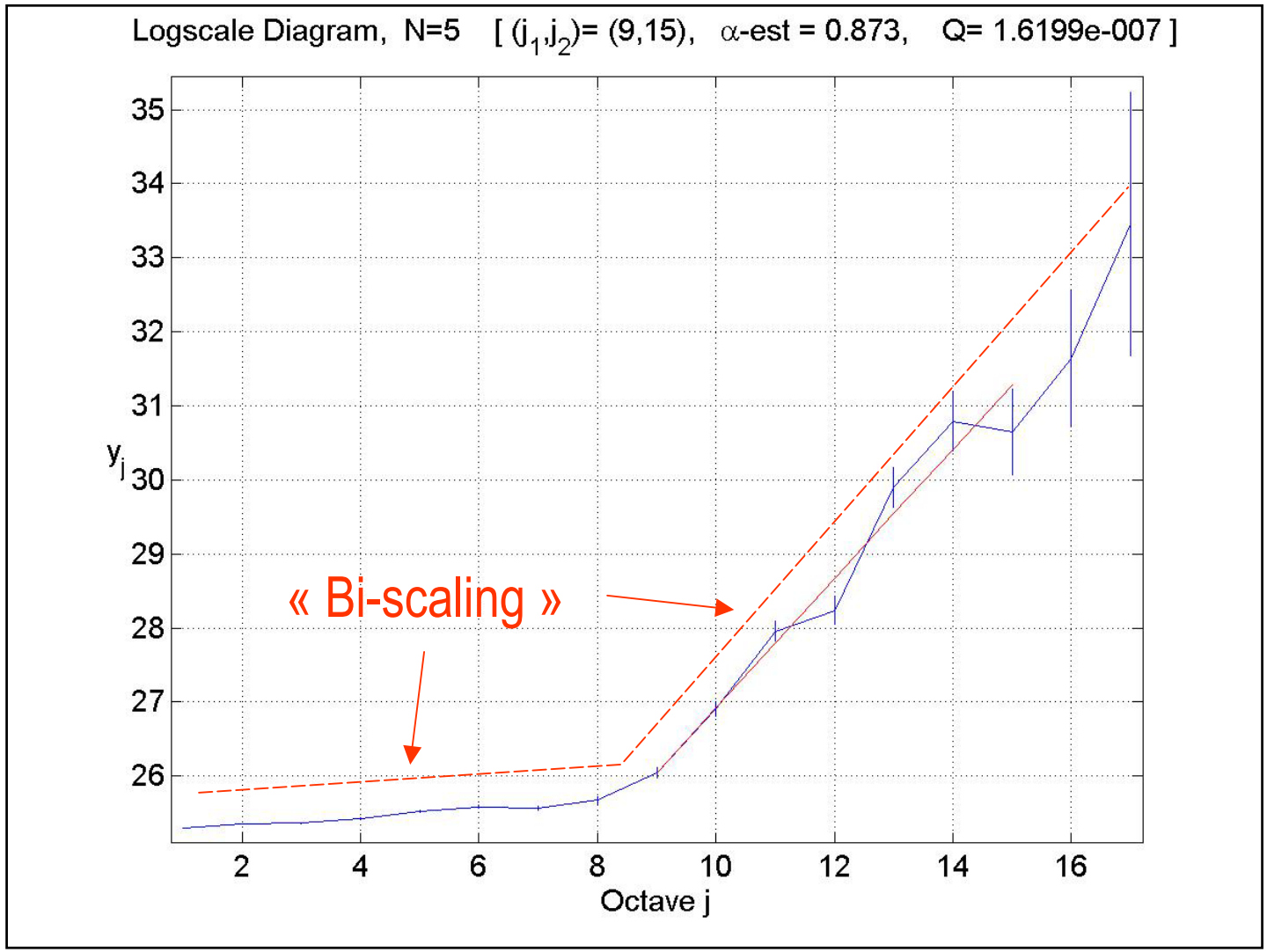
- Suspicion of Self-similarity
- Variability of traffic profile at all scale is a major matter for:
  - QoS
  - Stability
  - Performance
  - …

Analysis of traffic

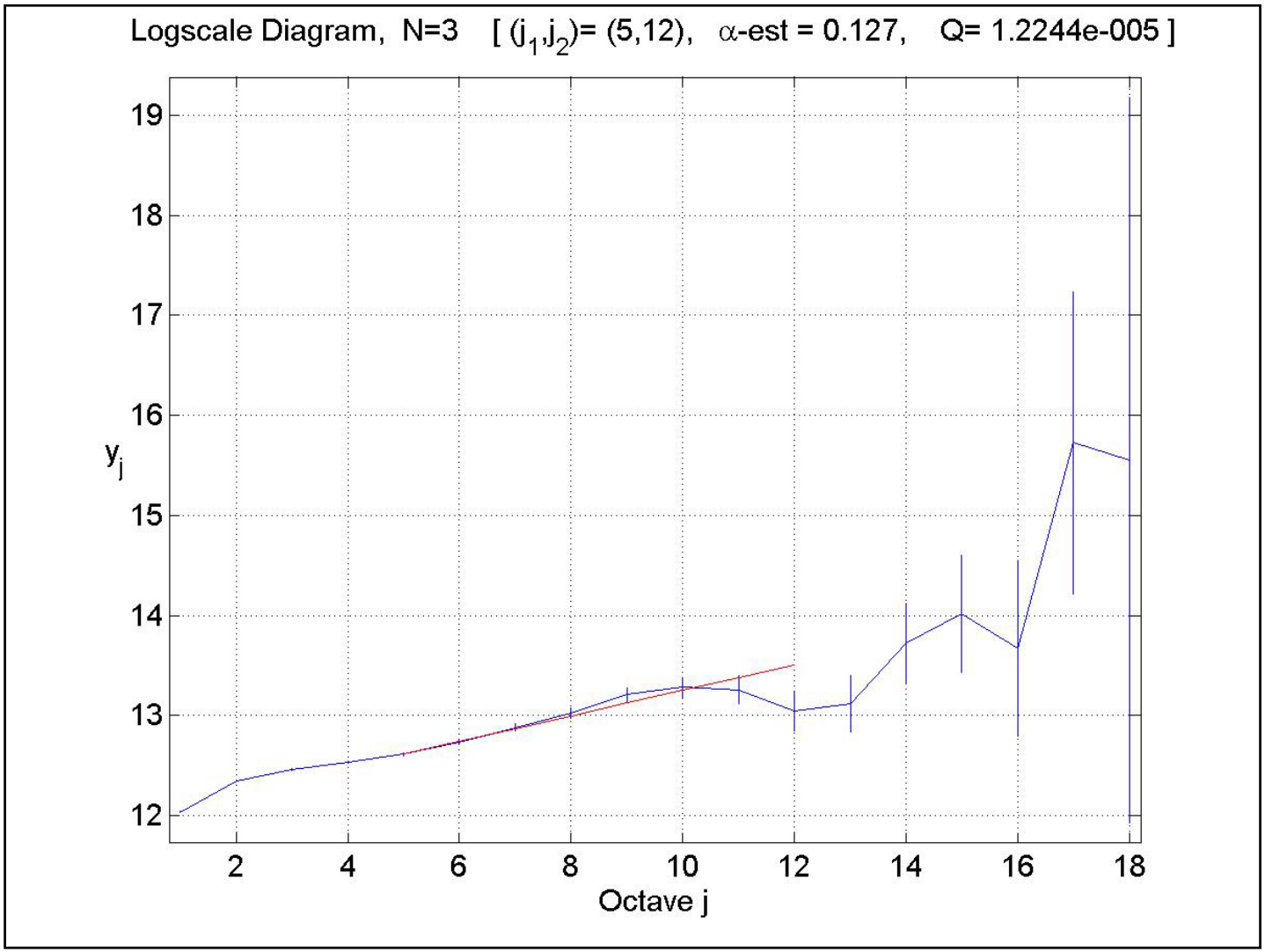
	Access traffic	Backbone traffic
Hurst (H) parameter	H = 0,915 [0.868, 0.962]	H = 0,561 [0.556, 0.565]

- Access traffic is very complex
- Backbone traffic is smoother
- Networking main issues (QoS, performance decrease,…) mainly appear on edge and / or access links

LRD measurements for edge network



LRD measurements for core backbone



Conclusion on traffic modeling

- Backbone traffic is almost Poisson
- Edge Traffic then is not Self-similar

- But LRD is really an issue
- Most effort has to be put on edge network

More information about METROPOLIS

http://www-rp.lip6.fr/metrologie

http://www.laas.fr/~owe/METROPOLIS/metropolis.html