Experimentation driven traffic monitoring and engineering research

Amir KRIFA (Amir.Krifa@sophia.inria.fr)

Outline

i. Future directions of Internet traffic monitoring and engineering
ii. Experimental limitations
iii. Our platform as an answer to these limitations
iv. Some validations results
v. Summary

Outline

i. Future directions of Internet traffic monitoring and engineering

ii. Experimental limitations

iii. Our platform as an answer to these limitations

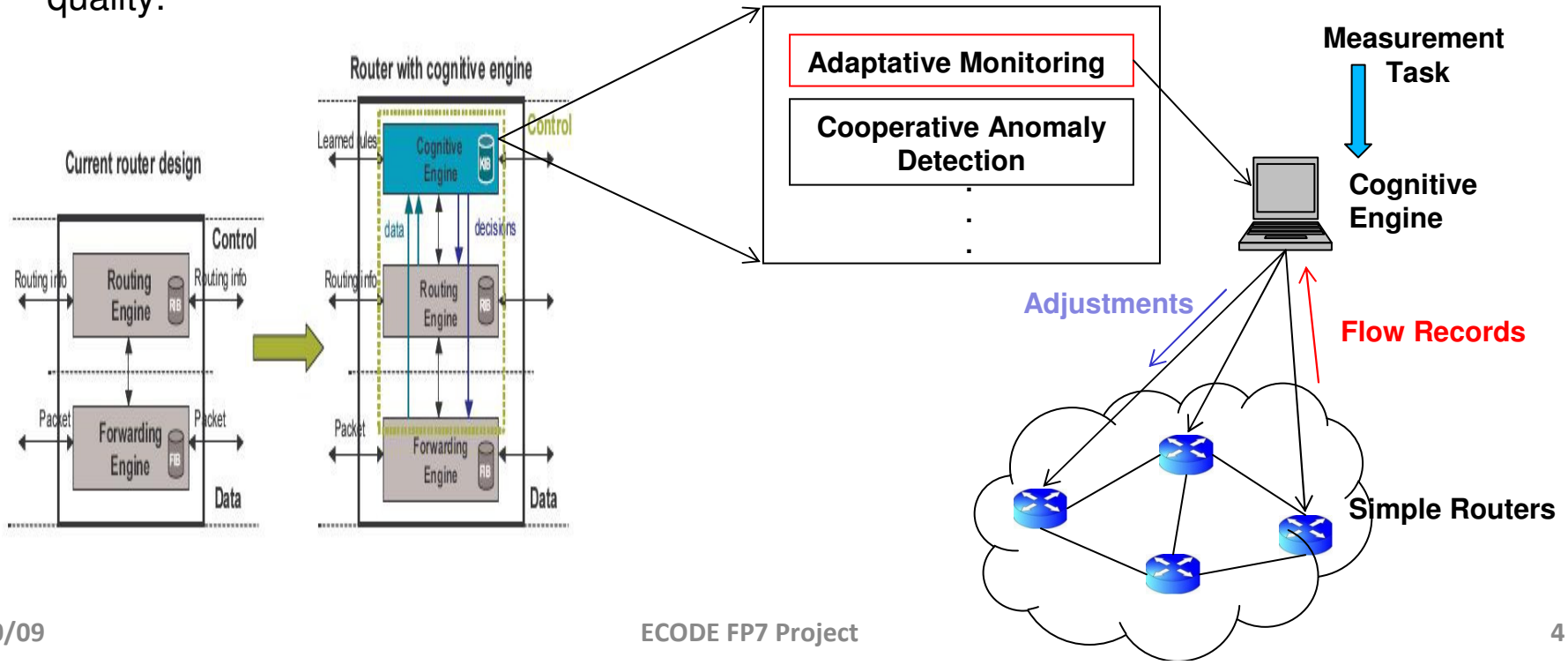
iv. Some validations results

v. Summary

Future directions of Internet Traffic Monitoring and Engineering

Introducing the ECODE project as a future direction: Experimental COgnitive Distributed Engine

- Develop and validate experimentally a **COGNITIVE** monitoring and routing system,
- Combining both networking and machine learning research fields.
- Meet the challenges experienced by the Internet in terms of manageability and security, availability and accountability, as well as routing system scalability and quality.



Outline

i. Future directions of Internet traffic monitoring and engineering

ii. Experimental limitations

iii. Our platform as an answer to these limitations

iv. Some validations results

v. Summary

Limitations of available experimentation facilities

Towards testing the new algorithms related to our adaptative monitoring solution,

- Most ISP(s) does not accept to provide real time control on large number of real monitors (mainly for privacy and security reasons).
- Using network emulators coupled with synthetic traffic generators and monitoring tools, exp: using Emulab + YAF (Flow meter)
  - Lack of traffic realism and scaling to large topologies costs a lot.
- Parsing and studying real traffic traces collected on specific links.
  - No online adaptative control available !

So, how can we test and validate our adaptative monitoring solution ?

Outline

i. Future directions of Internet traffic monitoring and engineering

ii. Experimental limitations

iii. Our platform as an answer to these limitations

iv. Some validations results

v. Summary

The objectives behind our Platform

Objectives: Providing a new approach for the emulation of real Internet traffic and for its monitoring across the different routers.

We put at the disposal of users:

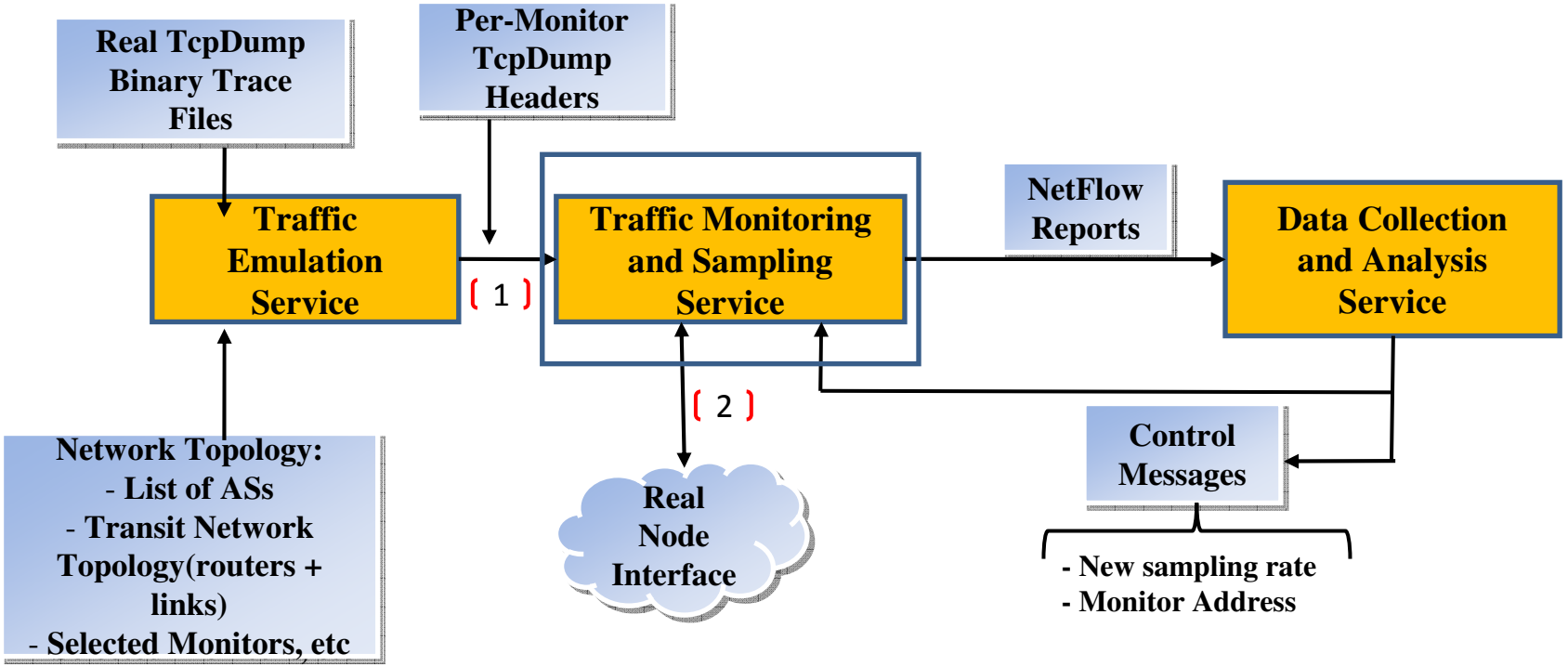
- A real traffic emulation service

- A set of libraries and tools capable of Cisco NetFlow data export and collection & analysis,

Which are meant to run advanced applications for network wide monitoring and optimization.

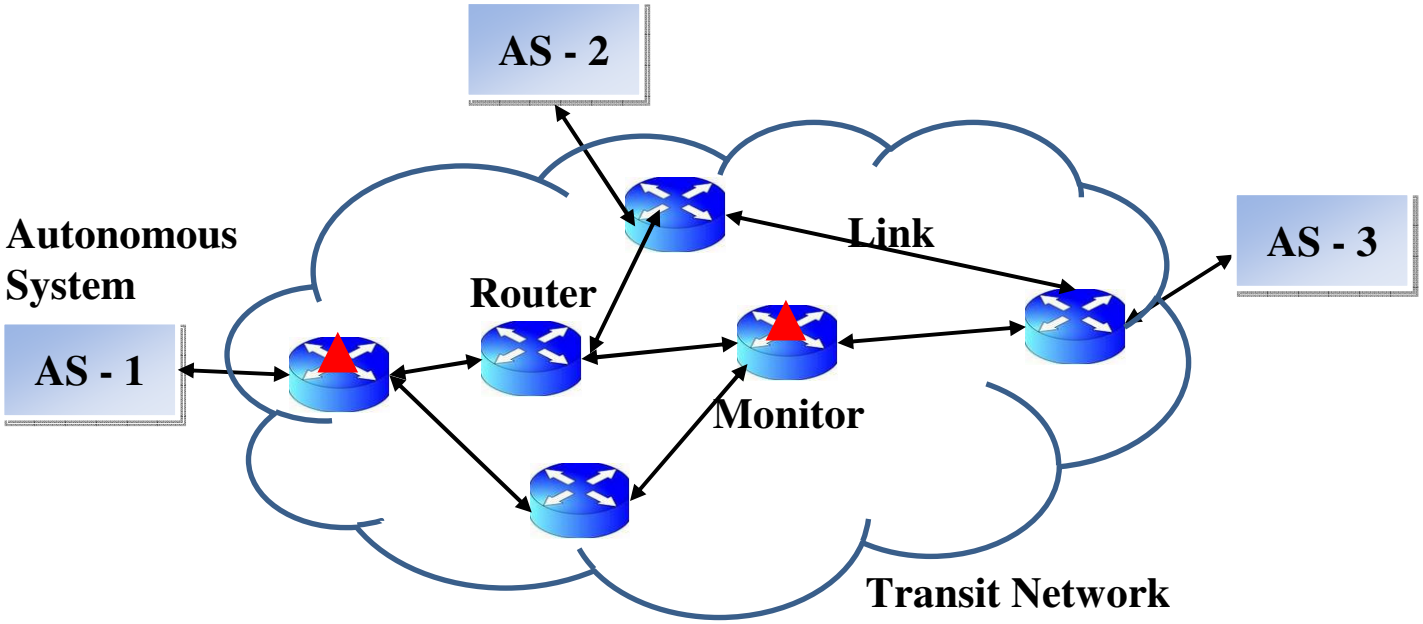
Architecture of our Platform

- Starting from a set of collected real traces (either from a single point during different periods of time or from different points)
- Given a network topology composed of virtual routers and links but real monitors
- Plays the real traces (not synthetic) within the given topology while providing remote-controllable traffic monitoring and sampling capabilities for each router



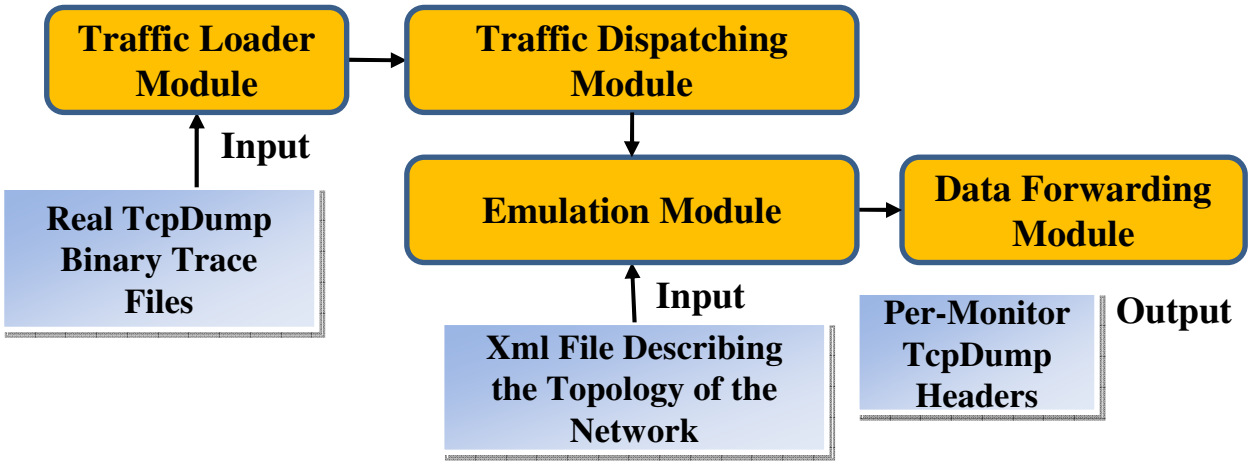
Example of an Emulated Topology

- **Through** XML Configuration files,
  - **Link' characteristics:** Capacity, Delay, Cost
  - **AS' characteristics:** Weight, Edge router,
  - **Router' characteristics:** Interfaces, Interfaces' monitoring status, Links, …



- We provide as much details as it is needed to re-produce the closest possible topology to the real one. An example of XML schema is available at http://planete.inria.fr/GEANT.

Traffic Emulation Service



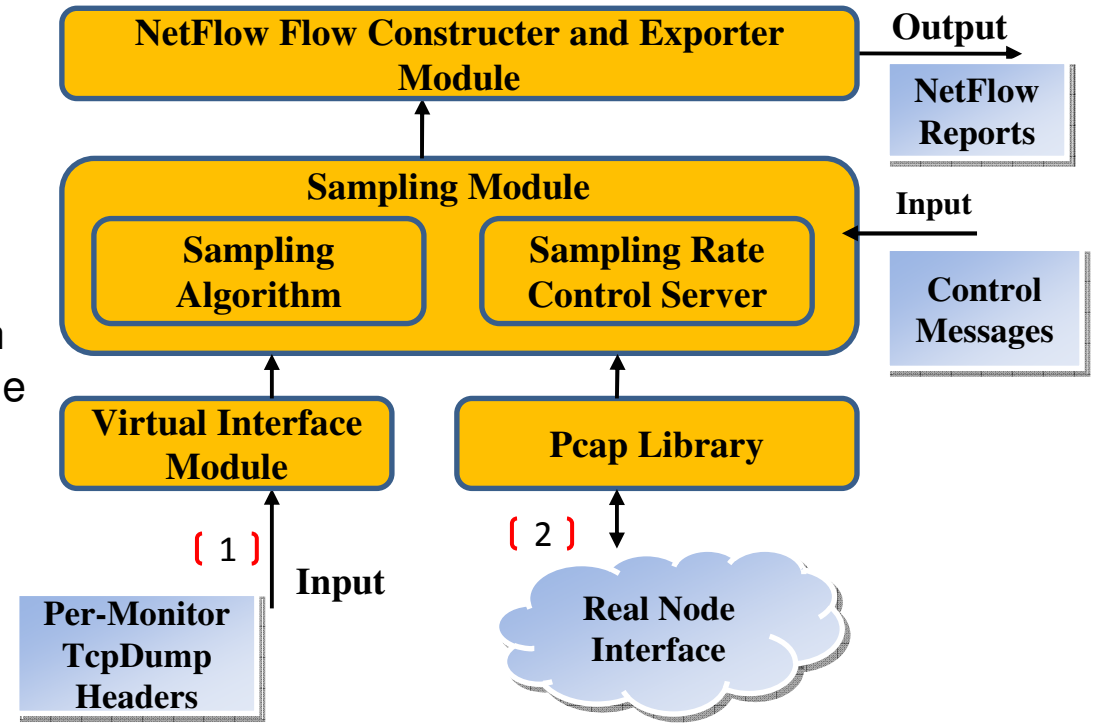
- **Dispatching algorithm: Weighted Random** based on one hand on the list of weights that the user associates to the different ASes and on another hand on the prefix length specified by the user (/16, /24, etc)
  - All IP addresses of a prefix are put in the same AS
- **The four modules run in parallel** so as to minimize the memory footprint, enable the emulation to scale to big topologies (example: GEANT's backbone topology) and prevent the introduction of latency while scheduling packets
- **Routing Algorithm:** Routes are static and set according to the Dijkstra algorithm to the shortest routes, then passed in the XML configuration file (other routing possible)

Traffic Monitoring and Sampling Service

➢ **Sampling algorithm:** If a user chooses a sampling rate of **A**/**B** (**A** packets among **B** packets, **A < B**, **B > 0**, **A >= 0**), then every **B** packets, the sampling module generates randomly a set **S** of **A** numbers within the interval **[1, B]**. Packets with numbers outside the set **S** are rejected and only the remaining packets are considered for 5-tuple flow construction.

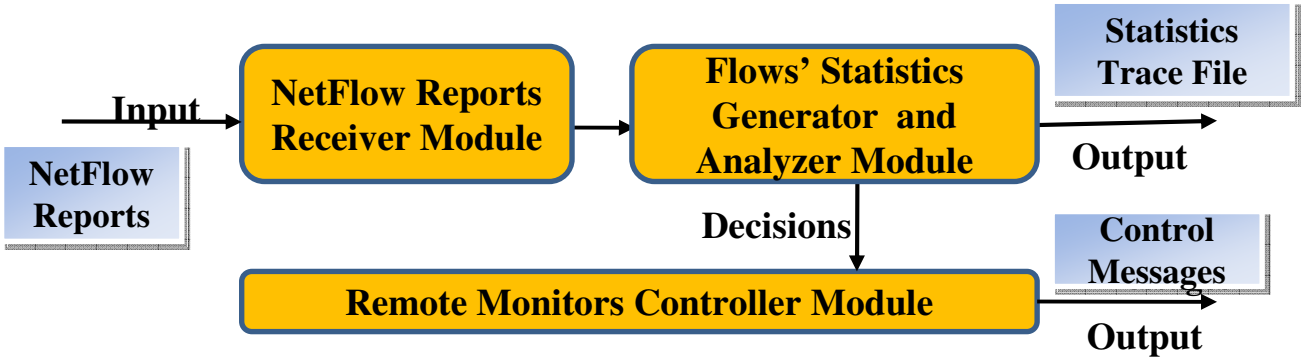
➢ **Sampling Rate Control server:** Enables to remotely control the sampling rate.

➢ **Flow Constructor and Exporter:** constructs 5-tuple flows starting from sampled packets, merges them within NetFlow reports and sends them to the Collector.



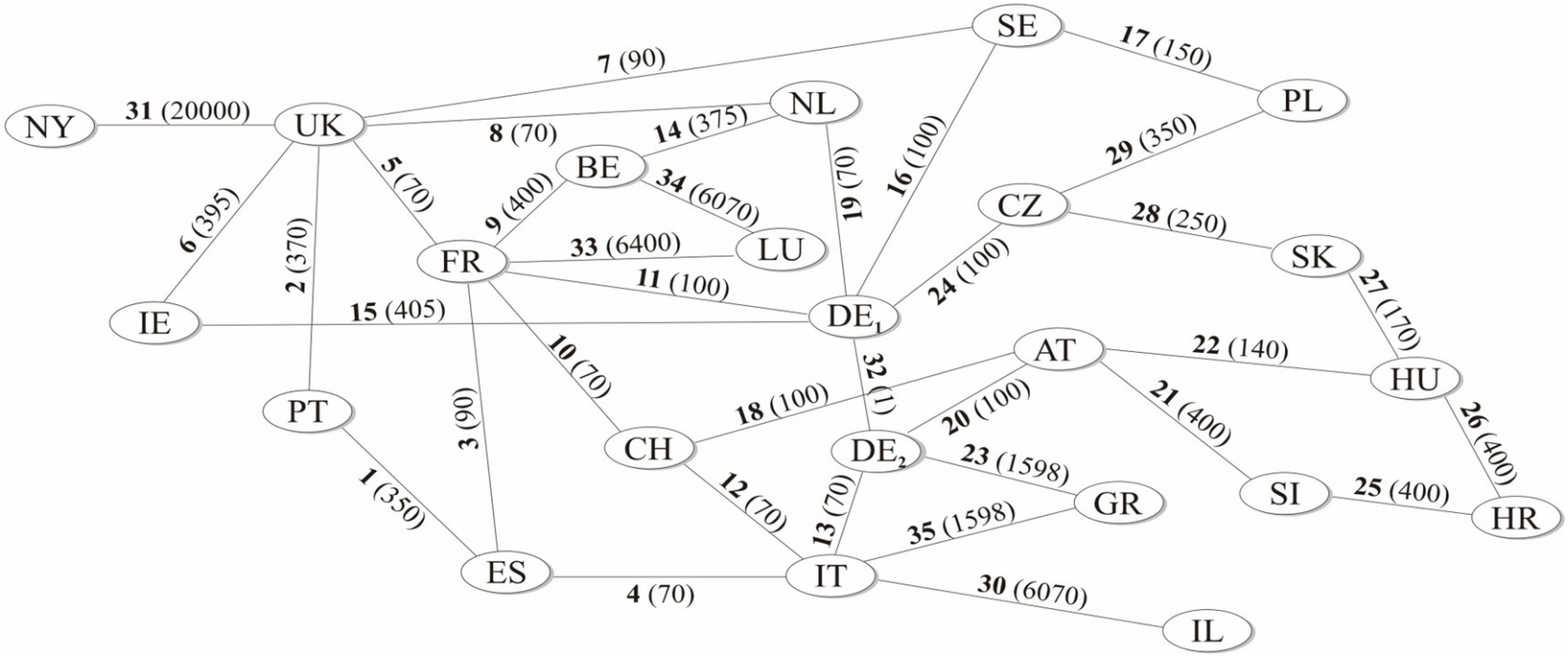
Data Collection and Analysis Service

- **NetFlow reports receiver module:** Receives and decodes the reports sent by the traffic monitoring and sampling service.
- **Flow statistics generator and analyzer module**: Calculates statistics on flows from the collected reports (number of packets/flow, etc) and replies to application questions. It implements the cognitive engine responsible of the decisions on changing the sampling rates in the monitors for measurement accuracy optimization.
- **Remote monitor controller module**: Sends control messages (new sampling rate, monitor address) to **the sampling rate control server** within the **traffic monitoring and sampling service** in order to change the monitor sampling rate.



Possible Experimentation Scenario

- **Emulated Topology:** Inspired from the GEANT's backbone topology
  - 23 routers, 97 interfaces, XML file at http://planete.inria.fr/GEANT/
- **Real Traffic Traces:** Taken from the MAWI Working Group Traffic Archive
- **Dispatching Algorithm:** The weight of an AS proportional to the speed of its access link



Outline

i. Future directions of Internet traffic monitoring and engineering

ii. Experimental limitations

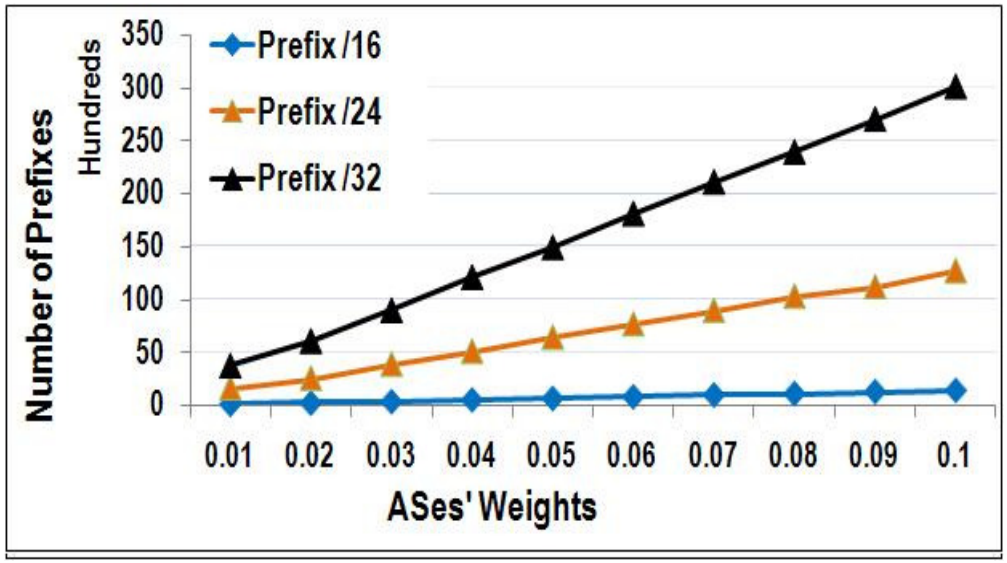
iii. Our platform as an answer to these limitations

iv. Some validations results

v. Summary

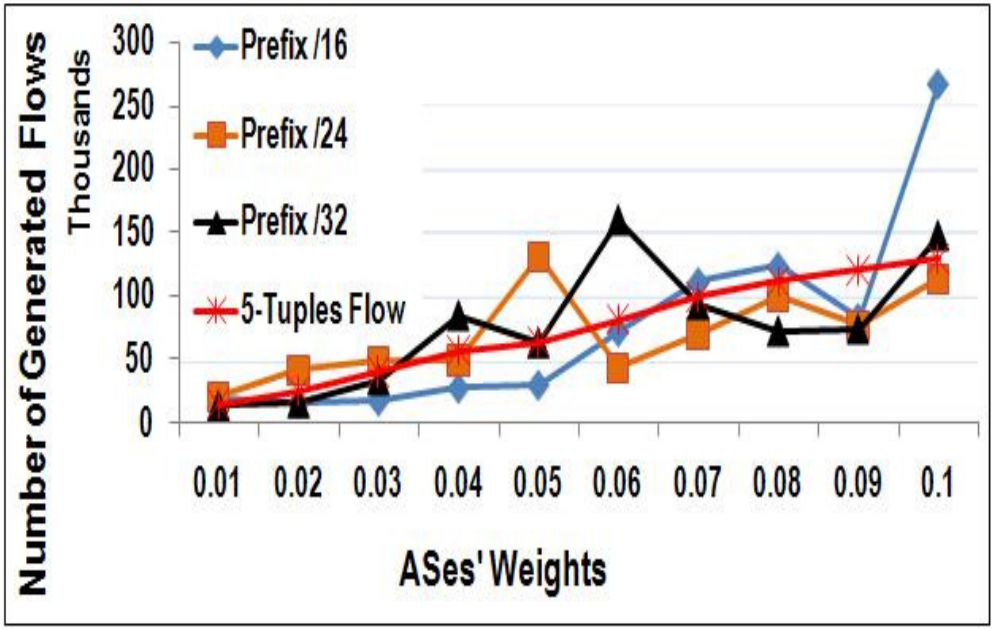
Studying the effectiveness of the dispatching mechanism

Does each AS generate as much traffic as the importance of the weight associated to it?



The resulting curves remain linear for different prefix lengths. So, we conclude that our emulator dispatches the prefixes to ASes without any bias.

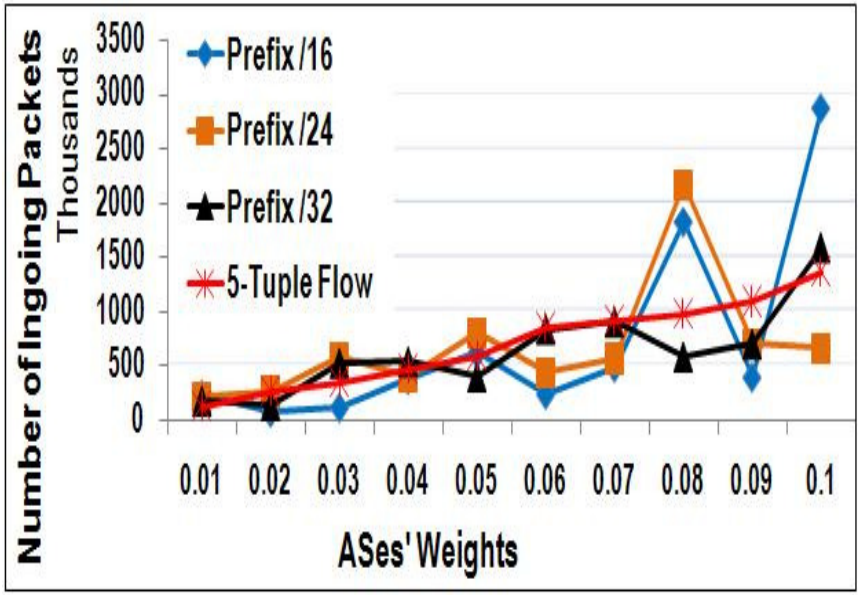
Studying the effectiveness of the dispatching mechanism

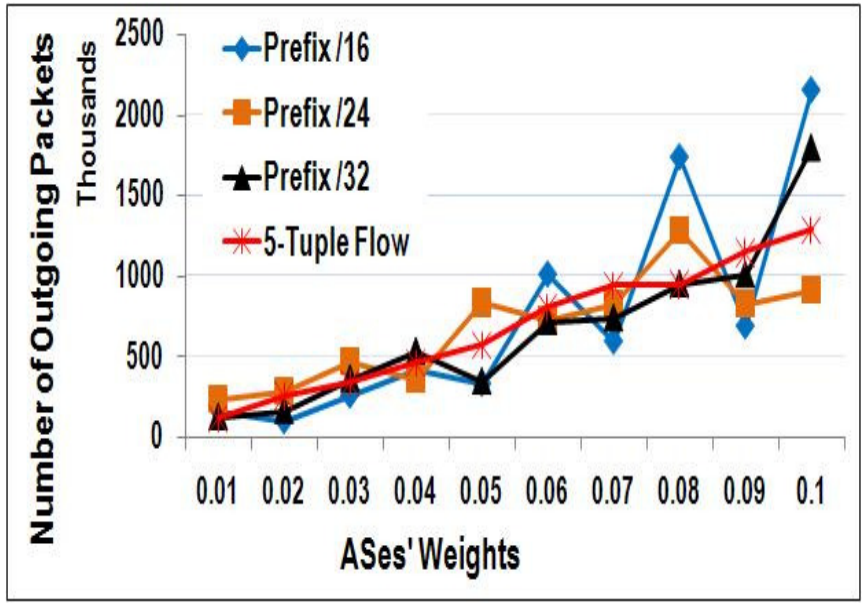


Number of generated flows by different ASes Having different weights

- The number of generated flows scale with the AS weights but do not fit a perfect line. Nevertheless, the fitting improves when the prefix granularity becomes finer.
- This indeed comes from the presence of very large prefixes of different volumes that, when dispatched over the ASes, cause such deviations in the traffic; the coarser the prefix the more important this phenomenon.

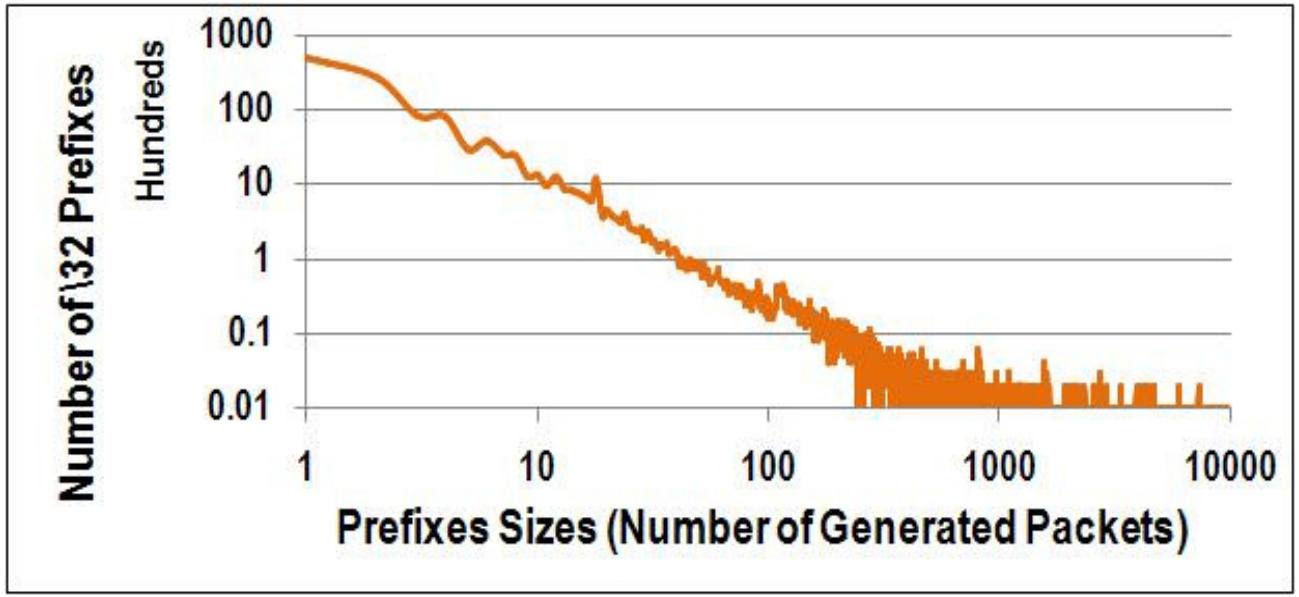
Studying the effectiveness of the dispatching mechanism





Number of ingoing/outgoing packets for ASes Having different weights

Studying the effectiveness of the dispatching mechanism



➢ Clearly, there is a **power-law** behavior leading to very large prefixes compared to the average prefix size (these are servers, heavy users, etc).

Outline

i. Future directions of Internet traffic monitoring and engineering

ii. Experimental limitations

iii. Our platform as an answer to these limitations

iv. Some validations results

v. Summary

Summary

- Described our platform for network wide traffic sampling and monitoring (Traffic emulation service, Traffic monitoring and sampling service and Data collection and analysis service)

- Our platform offers a complete set of features towards the development and evaluation of solutions for network monitoring and management.

  - The possibility to reproduce real backbone network topology,

  - To monitor and sample the packets being forwarded in a given router,

  - And finally the ability to analyze the collected flows and reconfigure the monitoring points accordingly towards the achievement of a given task.

http://planete.inria.fr/NWTSM