Inter-Providers Traffic Analyzer

Mix s.r.l. - Padova Ricerche

RIPE 46, 1-5 September, Amsterdam

Agenda

- Objective
- Architecture
- Anomaly detection

Objective

- Monitoring the incoming and outgoing traffic of the ISPs connected to an IX
  - to detect anomalies and failures
  - analyzing the traffic at the physical layer

Architecture

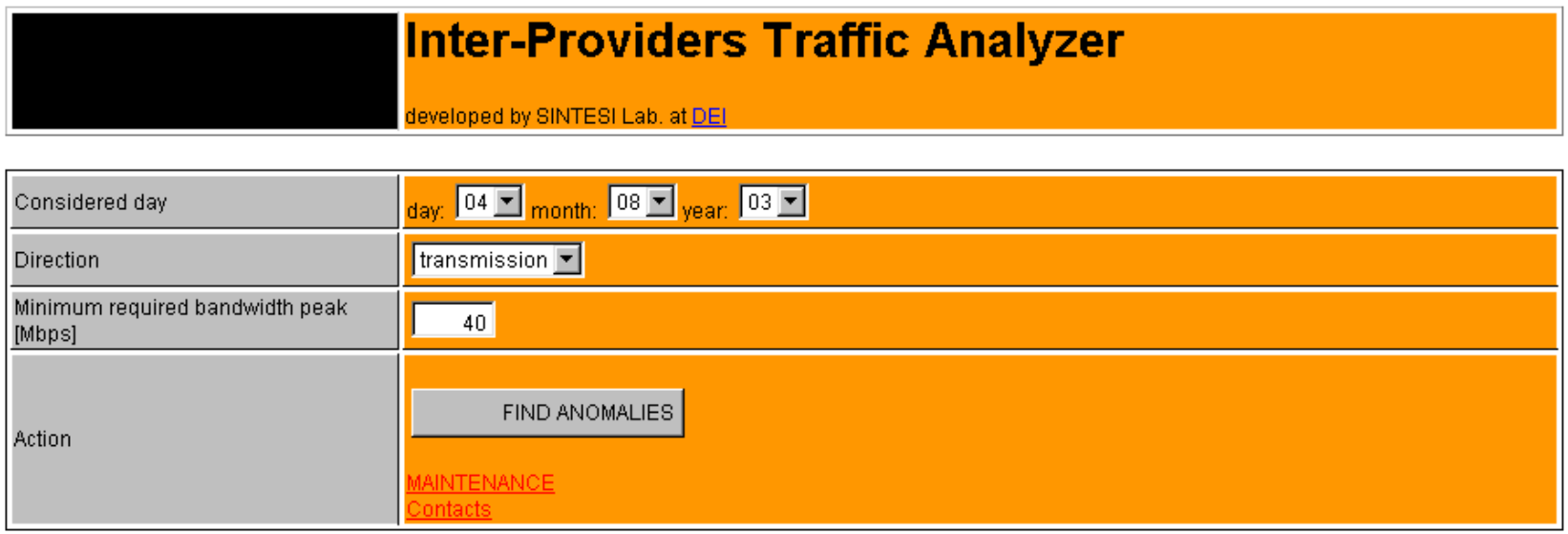
- Acquisition module
  - SNMP & PostgreSQL
- Computation module
  - Matlab
- Web interface
  - PHP
- Mail reporting system

Computation module

- It calculates:
  - Typical traffic intensity curve
  - Current traffic intensity curve
  - Mean square errors
  - Anomaly score
  - Correlation between anomalies

Anomaly detection

- The starting form:



Inter-Providers Traffic Analyzer

developed by SINTESI Lab. at DEI

Considered day	day: 04 month: 08 year: 03
Direction	transmission
Minimum required bandwidth peak [Mbps]	40
Action	FIND ANOMALIES MAINTENANCE Contacts

Anomaly detection

- The “anomaly scores” table:

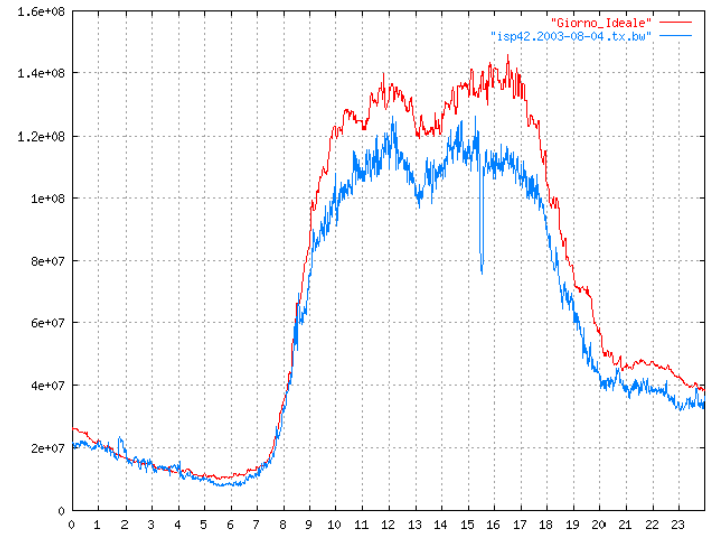
Interface	Max bandwidth (Mbps)	0:0	1:0	2:0	3:0	4:0	5:0	6:0	7:0	8:0	9:0	10:0	11:0	12:0	13:0	14:0	15:0	16:0	17:0	18:0	19:0	20:0	21:0	22:0	23:0
interbusiness [0]	649.46	0.02 0.02 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.00	0.02 0.01 0.05 0.01	0.00 0.01 0.01 0.00	0.01 0.01 0.02 0.01	0.02 0.01 0.01 0.02	0.01 0.03 0.02 0.03	0.02 0.03 0.04 0.01	0.02 0.02 0.02 0.02	0.04 0.03 0.01 0.02	0.03 0.02 0.02 0.02	0.02 0.02 0.02 0.02	0.02 0.03 0.05 0.03	0.02 0.06 0.07 0.02	0.03 0.03 0.04 0.01	0.03 0.02 0.02 0.02	0.03 0.03 0.02 0.02	0.02 0.03 0.01 0.01	0.02 0.02 0.02 0.02	0.02 0.04 0.01 0.01	0.02 0.01 0.01 0.02	0.01 0.02 0.01 0.02
fastweb [3]	115.20	0.04 0.04 0.02 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.00 0.01 0.01 0.02	0.01 0.00 0.00 0.00	0.01 0.00 0.00 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.02 0.01 0.01 0.02	0.02 0.03 0.09 0.03	0.04 0.01 0.03 0.01	0.03 0.05 0.04 0.05	0.03 0.02 0.03 0.02	0.02 0.03 0.03 0.03	0.02 0.02 0.02 0.01	0.03 0.01 0.03 0.02	0.01 0.05 0.04 0.02	0.02 0.03 0.02 0.01	0.02 0.01 0.03 0.01	0.01 0.04 0.01 0.01	0.01 0.01 0.02 0.02	0.04 0.02 0.02 0.02	0.05 0.01 0.01 0.02	0.01 0.01 0.03 0.02
sw2-sw1-1 [39]	481.22	0.01 0.00 0.01 0.01	0.01 0.01 0.01 0.01	0.00 0.01 0.00 0.00	0.00 0.00 0.00 0.00	0.01 0.00 0.00 0.01	0.01 0.00 0.00 0.01	0.00 0.01 0.01 0.01	0.00 0.01 0.01 0.01	0.01 0.01 0.02 0.03	0.01 0.02 0.02 0.02	0.01 0.01 0.02 0.03	0.02 0.01 0.02 0.02	0.01 0.01 0.03 0.01	0.05 0.01 0.01 0.02	0.02 0.01 0.03 0.01	0.02 0.06 0.06 0.01	0.01 0.01 0.02 0.01	0.02 0.01 0.01 0.01	0.02 0.02 0.02 0.01	0.01 0.03 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.02 0.01 0.00	0.01 0.01 0.01 0.02	0.02 0.02 0.02 0.01
tiscali2 [40]	212.99	0.01 0.01 0.01 0.01	0.00 0.01 0.01 0.01	0.00 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.02 0.01 0.01 0.01	0.01 0.01 0.00 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.00	0.02 0.04 0.02 0.02	0.02 0.01 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.03 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.03 0.02	0.02 0.05 0.01 0.06	0.02 0.02 0.02 0.02	0.02 0.02 0.02 0.01	0.01 0.02 0.03 0.01	0.01 0.01 0.02 0.01	0.02 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.03 0.01
interbusiness2 [41]	265.90	0.02 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.00 0.01 0.00 0.01	0.01 0.00 0.01 0.00	0.01 0.01 0.01 0.01	0.01 0.01 0.02 0.00	0.00 0.01 0.00 0.00	0.01 0.00 0.01 0.01	0.00 0.01 0.01 0.01	0.02 0.00 0.01 0.02	0.01 0.01 0.01 0.01	0.02 0.02 0.02 0.00	0.01 0.01 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01
albacom [42]	126.25	0.01 0.01 0.00 0.01	0.00 0.00 0.00 0.02	0.00 0.01 0.01 0.01	0.01 0.00 0.01 0.00	0.02 0.00 0.00 0.00	0.00 0.00 0.00 0.00	0.00 0.00 0.01 0.00	0.01 0.00 0.02 0.02	0.01 0.04 0.04 0.03	0.05 0.02 0.02 0.01	0.03 0.02 0.06 0.02	0.03 0.04 0.05 0.05	0.04 0.02 0.01 0.02	0.03 0.05 0.03 0.03	0.02 0.04 0.04 0.03	0.06 0.21 0.25 0.04	0.02 0.03 0.04 0.05	0.03 0.02 0.02 0.03	0.04 0.01 0.03 0.01	0.01 0.04 0.02 0.01	0.03 0.01 0.02 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.00
i.net2 [43]	121.48	0.01 0.01 0.01 0.03	0.01 0.01 0.00 0.01	0.01 0.01 0.01 0.00	0.00 0.01 0.00 0.01	0.01 0.01 0.00 0.02	0.04 0.01 0.01 0.01	0.01 0.00 0.02 0.01	0.01 0.01 0.02 0.02	0.03 0.14 0.03 0.02	0.03 0.02 0.03 0.03	0.02 0.04 0.02 0.03	0.02 0.02 0.01 0.04	0.02 0.02 0.03 0.03	0.03 0.02 0.03 0.03	0.02 0.03 0.05 0.04	0.02 0.04 0.04 0.04	0.03 0.01 0.02 0.04	0.03 0.02 0.04 0.01	0.01 0.02 0.02 0.02	0.01 0.01 0.03 0.01	0.02 0.02 0.01 0.01	0.02 0.01 0.01 0.01	0.01 0.01 0.01 0.04	0.01 0.02 0.05 0.05
infostrada [44]	296.57	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.01	0.01 0.00 0.01 0.00	0.00 0.00 0.00 0.00	0.00 0.00 0.00 0.02	0.03 0.01 0.01 0.01	0.01 0.01 0.03 0.01	0.01 0.02 0.01 0.01	0.01 0.01 0.02 0.03	0.03 0.01 0.02 0.01	0.03 0.01 0.01 0.02	0.02 0.01 0.01 0.02	0.03 0.03 0.03 0.01	0.01 0.03 0.02 0.02	0.01 0.01 0.01 0.02	0.03 0.02 0.01 0.01	0.01 0.02 0.01 0.02	0.02 0.06 0.02 0.03	0.02 0.01 0.02 0.02	0.02 0.03 0.02 0.01	0.01 0.01 0.01 0.01	0.01 0.02 0.01 0.01	0.01 0.02 0.01 0.02	0.01 0.01 0.02 0.01
swisscomip [57]	84.04	0.02 0.02 0.01 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.01 0.01	0.01 0.01 0.01 0.00	0.01 0.01 0.01 0.05	0.02 0.02 0.01 0.01	0.03 0.02 0.01 0.01	0.02 0.01 0.02 0.02	0.03 0.02 0.01 0.02	0.01 0.03 0.01 0.01	0.02 0.00 0.03 0.02	0.02 0.02 0.02 0.03	0.01 0.03 0.03 0.06	0.04 0.01 0.01 0.02	0.03 0.04 0.02 0.03	0.03 0.01 0.02 0.04	0.01 0.04 0.03 0.02	0.01 0.02 0.02 0.01	0.02 0.01 0.03 0.02	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.02	0.03 0.03 0.02 0.02	0.02 0.02 0.01 0.01	0.02 0.01 0.06 0.06

Anomaly detection

- The traffic intensity curves:

Anomalies for interface albacom [42] tx on 4 Aug 2003

Click here to see traffic in opposite direction



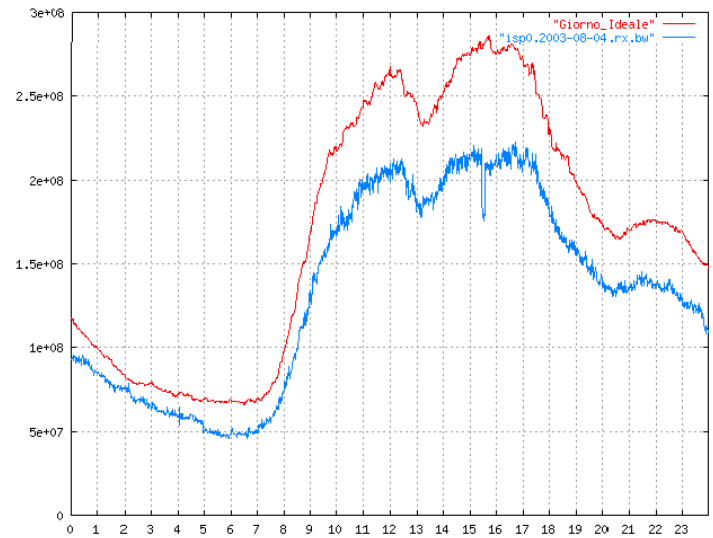
Max bandwidth	0:0	1:0	2:0	3:0	4:0	5:0	6:0	7:0	8:0	9:0	10:0	11:0	12:0	13:0	14:0	15:0	16:0	17:0	18:0	19:0	20:0	21:0	22:0	23:0
126.25	0.01 0.01 0.00 0.01	0.00 0.00 0.00 0.02	0.00 0.01 0.01 0.01	0.01 0.00 0.01 0.00	0.02 0.00 0.00 0.00	0.00 0.00 0.00 0.00	0.00 0.00 0.01 0.00	0.01 0.00 0.02 0.02	0.01 0.04 0.04 0.03	0.05 0.02 0.02 0.01	0.03 0.02 0.06 0.02	0.03 0.04 0.05 0.05	0.04 0.02 0.01 0.02	0.03 0.05 0.03 0.03	0.02 0.04 0.04 0.03	0.06 0.21 0.25 0.04	0.02 0.03 0.04 0.05	0.03 0.02 0.02 0.03	0.04 0.01 0.03 0.01	0.01 0.04 0.02 0.01	0.03 0.01 0.02 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.00
I° quarto																edisontel								
II° quarto																albacom								
III° quarto											interbusiness kpnqwestitalia					interbusiness sw1-sw2-1 albacom								
IV° quarto												blixer												

Anomaly detection

- A correlated anomaly in another ISP:

Anomalies for interface interbusiness [0] rx on 4 Aug 2003

Click here to see traffic in opposite direction



Max bandwidth	0:0	1:0	2:0	3:0	4:0	5:0	6:0	7:0	8:0	9:0	10:0	11:0	12:0	13:0	14:0	15:0	16:0	17:0	18:0	19:0	20:0	21:0	22:0	23:0
223.17	0.02 0.01 0.01 0.00	0.01 0.01 0.01 0.01	0.01 0.00 0.00 0.01	0.01 0.01 0.00 0.01	0.01 0.01 0.01 0.02	0.00 0.00 0.01 0.00	0.01 0.00 0.02 0.00	0.02 0.01 0.01 0.01	0.02 0.03 0.03 0.02	0.03 0.01 0.02 0.02	0.03 0.03 0.06 0.03	0.02 0.02 0.01 0.02	0.02 0.03 0.06 0.02	0.03 0.02 0.02 0.01	0.02 0.03 0.02 0.03	0.01 0.17 0.17 0.03	0.02 0.03 0.04 0.02	0.02 0.05 0.04 0.03	0.03 0.02 0.02 0.01	0.02 0.01 0.02 0.02	0.01 0.01 0.02 0.01	0.01 0.01 0.02 0.01	0.01 0.02 0.02 0.02	0.02 0.02 0.02 0.03
I° quarto																interbusiness colt-italia mc-link sw2- sw1-1 garr2								
II° quarto																								
III° quarto											albacom		blixer globalcrossing colt-italia			interbusiness blixer easynet sw2- sw1-1 albacom								
IV° quarto																								

Conclusions

- We and 4 ISP are testing the tool
- Software availabilty & more info:
  - 3rd Euro-IX Forum, 3-4 November 2003 Lisbon Portugal
  - mail to: matheo.labanti@mix-it.net