TRAMMS – TRAFFIC MEASUREMENTS AND MODELS IN MULTI-SERVICE NETWORKS

MILESTONE M4.2 – IP TRAFFIC MONITORING BY MEANS OF TRAMMS DEVICES

Identifier:	Milestone M4.2
Class:	Report
Version:	V02
Version Date:	2009-10-14
Distribution:	Public
Responsible Partner:	TID
Editor:	Angel Ferreiro

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document describes the activities and achievements of different partners within WP4 until June, 2009. The aim of covering traffic monitoring in IP networks can be summarized as follows:

	QoS	Routing
Active	✔	
Passive	✔	✔

In the 2009 Celtic event, that took place in Paris on March 11-12, a couple of demos were presented about passive systems for QoS measurement and BGP routing repositories formation. The active QoS (bandwidth and network availability) systems developed by TRAMMS partners were already presented in the project MTR, on October, 23rd, in Bilbao (Spain).

The results of these works have been published in different congress and have contributed to ITU-T recommendations [1-3]; a new publication with a global updated presentation is intended to be submitted next month.

The systems described herein have followed an industrial path of development either independently or in association with other QoS supervision systems by Telefonica, Ericsson and a few SME in Spain (TELNET, GCM, HPCN).

A complex test-bed to integrate QoS measurement devices and make the Celtic event simulated results be part of a complete monitoring system in the Spanish academic network RedIris is currently under development, just waiting for this commercial network finish its works of updating infrastructures.

1 INTRODUCTION

This document summarises the results of TRAMMS as traffic measurement products for commercial applications. A more extensive description will be offered in Deliverable D4.3, together with a plausible exploitation plan and some examples of real use.

2 QoS ACTIVE PROBES

2.1 NETAUDITOR

The delay of packets to reach their destination is a first measure of QoS since its relevance for real time applications and side-effects to packet loss. Additionally, by means of filtering and extrapolating data, one can have a reasonable idea of the link availability or bandwidth that can still be used for datagrams transport.

Either p2p or mp2mp systems can be developed for this purpose. TELNET developed the NETAUDITOR system for p2p delay measurements which has been deployed in Telefonica commercial network for routine network analysis of performance. For a deep description of NETAUDITOR, refer to D4.2.

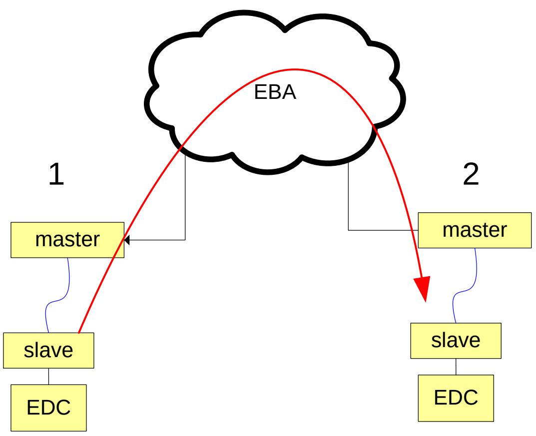

FIGURE 1: QoS measurement with netauditort

The NETAUDITOR system has been formatted for commercial utilization allowing to infer jitter, packet loss and packets out of order aside from latency with the following functional characteristics:

- Measurement over the whole path
- Constant monitoring in real time from the central offices
- Collection of historical statistics

When integrated in a framework of network supervision, NETAUDITOR helps a network operator to detect bottlenecks, as well as underused paths. In order to achieve this, TELNET has improved both hardware and software to gain speed of calculation (use of FPGA, for instance) and make the system OAM management compliant

2.2 BART

Ericsson has continued its work on Bandwidth Available in Real Time (BART) system and has presented an amendment to ITU-T (see [4]) about “Packet Performance Parameters for Optimization of Stream Repair Techniques” that relies on BART.

BART main contribution to QoS measurement has to do with latency monitoring but its algorithms and its Kalman filter performance allows the user to estimate bandwidth in real time without a heavy calculation infrastructure. A nice description of this self-induced congestion mechanism is also found in D4.2.

As depicted in fig. 2, BART can work in a mp2mp scenario but the measures it obtains are end-to-end.

FIGURE 2: BART active probing scheme

By means of an intelligent set up of “bart nodes” within a commercial network, the operator can estimate the available bandwidth in it network without congesting it all but just calculating differences between several sections that make up the link of interest.

The systems works continuously and reports link capacity in real time. A friendly user interface is being currently developed so as to present the product for service providers and network operators.

2.3 One Way Delay measurements based on GPS synchronization

Aside from the well known method of sending pings and measure the complete round back of the datagrams, a way to measure delays is just synchronizing source and destination hosts so that, by simply signalling time of departure and arrival, one can obtain delays, jitter, etc. of a one way travel. UAM- HPCN has developed two approaches for a *Common Time Source* synchronization based on GPS modules to monitor *One Way Delay* for SLA compliance purposes, with a trade-off between cost of the solution and its precision. On the one hand we have a software solution based on a Linux Kernel module that timestamps with high precision (in the order of µs.) packets on their arrival. This software solution has less precision than the hardware solution, but it has lower cost, as it would only need a conventional PC and a GPS module (see Figure 3).

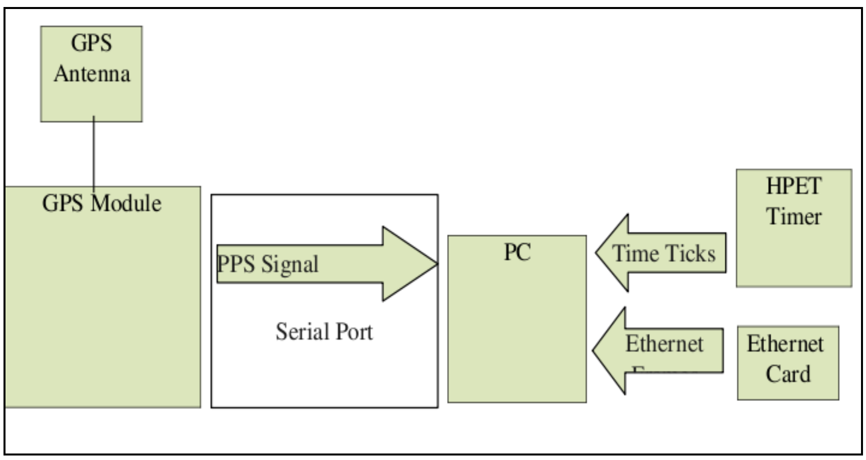

FIGURE 3: Software OWD monitoring solution

On the other hand there is a hardware based solution that makes use of a Field Programmable Gate Array and a Linux driver (see fig. 4). It is able to timestamp packets both on arrival and departure with an accuracy of nanoseconds, having also the advantage of being upgradeable to 10 Gbps.

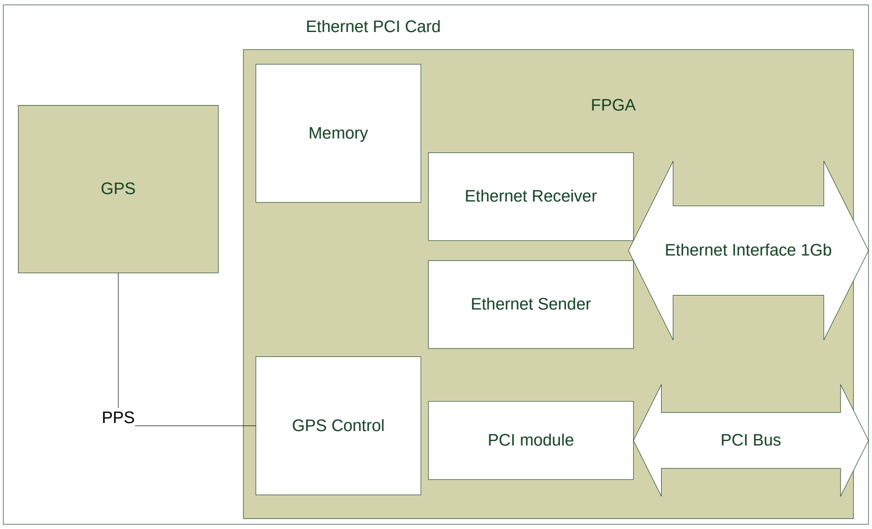

FIGURE 4: Hardware OWD monitoring solution

Both solutions are based on the same algorithms. UDP used for the measurement need not congestion the network and the results monitor the whole network performance in a standard way. No way to achieve high resolution in the sense that network operators can not analyse where the bottleneck is or how to improve the link but it is a very useful tool for service supervision and SLA survey: The need of eventually provide more bandwidth for a given service is pointed out in real time or simply logged for statistical process.

3 QoS PASSIVE PROBES

3.1 Gigabit Ethernet traffic analysis

Upon a similar hardware platform (FPGA based), UAM team is currently developing a passive probe for broadband traffic inspection. The initiative is supported by Telefonica aiming at installing these probes in its network for traffic analysis to discriminate web services, p2p traffic and other streaming services as a first step in introducing a differentiated QoS operation.

3.2 Deep packet inspection for broadband communications

DPI are a general software implemented solution for analysing traffic based on the protocols and/or inspection of packets heads to study whether sessions are established between a pair of hosts or if TCP mechanisms force many packets to be sent again form source to destination or simply the statistics of size, kind of services per hour, etc.

UAM has been analysing RedIris traffic data issued from netflow and that configuration (see fig. 5) can also be used for future deployments of passive probes in any real network.

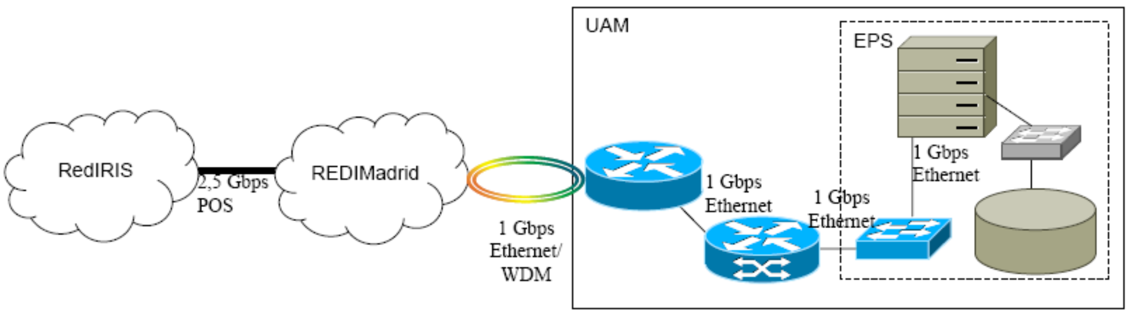

FIGURE 5: PASITO network configuration

In fact, TRAMMS WP2 has been fed by this set up as for the Spanish traffic data. However, more performing DPI are currently being implemented to gain speed and span its applications for different purposes.

4 ROUTING PASSIVE PROBES

4.1 Portable routing probe

TID and GCM have designed and built a prototype for BGP data extraction (see description in M4.1) aiming at collecting BGP data from different AS in a central system or repository (see fig. 6): The probe is directly linked to the border router which receives announces and routing tables from other routers (of other autonomous systems); the probe, in turn, sends those data to the repository at regular intervals.

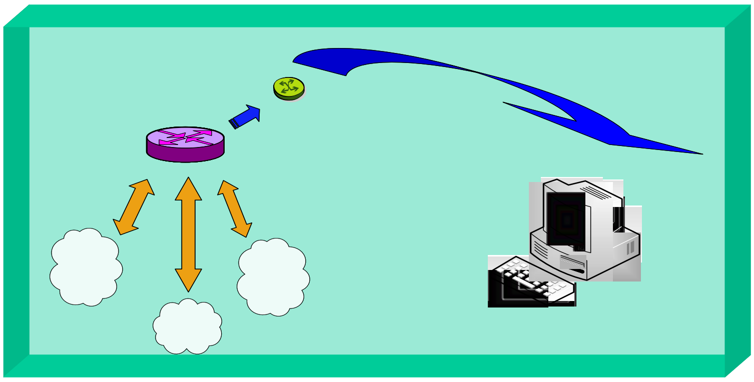

FIGURE 6: BGP routing data extraction

The probe software is based on the CVS branch of the Quagga routing. Some modifications to include automatic directory management, eliminate the need for external scripts for file compression and other improvements have been added. Thus a robust device has been achieved that serves as the basis for a BGP repository of very little cost that can be easily managed. A distribution of these BGP probes has been agreed with RedIris network for testing.

In 2009 Celtic event, a simulated network was used to demonstrate the benefits of the system (see fig.7)

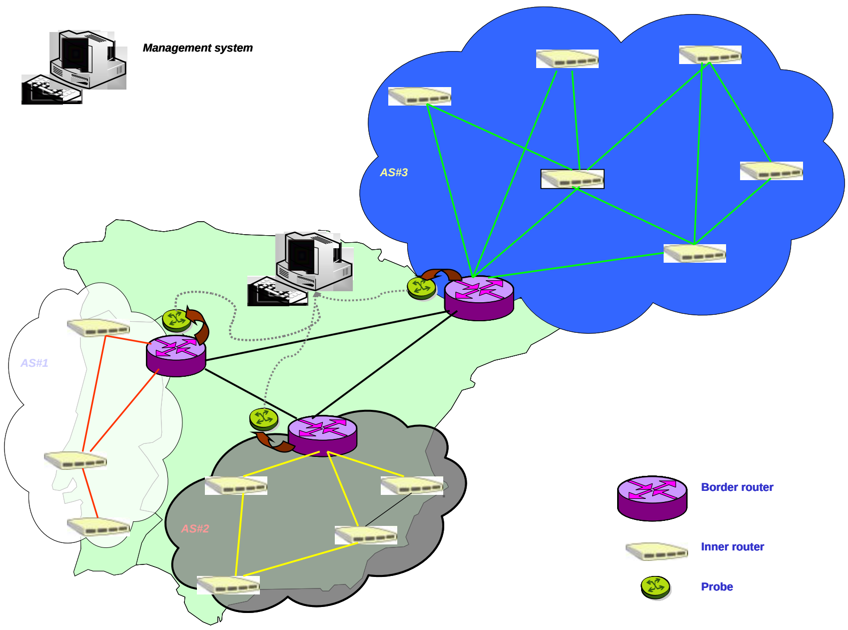

FIGURE 7: BGP repository for network configuration analysis and bottleneck elimination

Although a real test of these BGP probes for network analysis is still pending, a simple comparison of this “pocket” device for BGP repository with other already established (RIPE, for instance) would illustrate its advantages in terms of installation, and easy maintenance.

5 CONCLUSIONS

A good set of devices, software developments and test/bed designs, both for real and simulated networks have been produced in TRAMMS WP4 aiming at helping network operators and service providers to analyse and solve QoS troubles. More than half the prototypes issued from these efforts have already been applied for commercial purposes or are in the basis of industrial developments. Although the more ambitious goal of achieving guidelines to network management for bottlenecks elimination has not been reached, the momentum gained for traffic analysis and QoS monitoring deserves to be highlighted.