Wired/Wireless Internet Communications: 9th IFIP TC 6 International Conference, WWIC 2011, Vilanova i la Geltrú, Spain, June 15-17, 2011. Proceedings. Lecture Notes in Computer Science, Volumen 6649. Springer, 2011. 186-196.

DOI: http://dx.doi.org/10.1007/978-3-642-21560-5_16

Traffic monitoring for assuring quality of advanced services in Future Internet

A. Cuadra[1], F. Mata[2], J. L. García-Dorado[2], J. Aracil[2], J. López de Vergara[2], F. J. Cortés[3], P. Beltrán[3], E. de Mingo[3], A. Ferreiro[4]

[1]Indra Sistemas - Valladolid, Spain; [2]Universidad Autónoma de Madrid – Madrid, Spain; [3]Telnet Redes Inteligentes – La Muela, Spain; [4]Telefónica I+D – Madrid, Spain

acuadra@indra.es, felipe.mata@uam.es, jl.garcia@uam.es, javier.aracil@uam.es, jorge.lopez_vergara@uam.es, fcortes@telnet-ri.es, pbeltran@telnet-ri.es, edemingo@telnet-ri.es, olivo@tid.es

Abstract. Services based on packet switched networks are becoming dominant in telecommunication business and both operators and service providers must evolve in order to guarantee the required quality. Increasing bandwidth is no longer a viable solution because of the business erosion for network operators which cannot expect revenues due to the large investments required to satisfy new applications demand of bandwidth. This paper presents devices and a specific architecture of services monitoring platform that allows network operators and service providers to analyze the perceived quality of service and check their service level agreements. Thus, a cost-effective service management, based on direct IP traffic measuring, can be supported on integrated monitoring systems to provide network-centric mechanisms for differentiated quality of service, security and other advanced services.

Keywords: QoS, network monitoring, Future Internet.

1 Introduction

Future Internet must tackle the lack of built-in facilities to support non-basic functionalities in order to offer service-aware functionality [1]. Traditionally, the growth of the Internet and convergent services in the IP layer has been solved, as far as performance concerns, by increasing bandwidth and computational power in the edge devices. However, this trend is reaching its limits to provide Quality of Service (QoS); furthermore security and differentiated QoS, namely QoS as a service beyond the "best effort" packet delivery, which also takes into account specific applications characteristics, requires a new network-centric management architecture. Among their goals, the Future Internet service-aware architecture should include a cost-effective QoS management based on direct IP traffic monitoring so that network operators and

service providers can verify their Service Level Agreement (SLA). Besides, combining traffic measurement systems with on-line analysis will help detecting malicious users or unintended configuration errors even in multi-operator scenarios and render Internet governance plausible. In summary, the transition from specific circuit-switched (CS) networks towards convergent packet-switched (PS) networks supporting real-time applications and numerous new broad-band services in a disaggregated market must be based on powerful yet intelligent traffic monitoring systems in order to guarantee cost-effective QoS, security and privacy protection.
The objective is to keep the old CS networks facilities in the multiplexed Service Centric (SC) transport networks by means of additional control elements inside the network. So far only client devices and applications tackled these issues considering the operator could just offer them end-to-end (E2E) connectivity without any additional service. However, the required analysis to improve service architectures and diagnose configuration failures or critical dimensioning lacked significant traffic data from commercial networks. Numerous projects have developed measurement infrastructures to track Internet functioning [2] and several research groups have actively participated in these efforts [3], [4]. Recent proposals to use such measurement facilities for network management have raised relevant problems such as privacy protection, leading to the development of anonymization solutions [5]. Besides, the access to heterogeneous traffic monitoring data is very challenging; thus, a semantic tool (mediator) has been developed [6], and standardization initiatives [7] have been carried out in order to establish interoperable data formats, as well as KPI (key Performance Indicator) and other measurements to support QoS monitoring. This paper presents an architecture for service-aware networking compatible with Future Internet paradigms like resources virtualization and autonomic management within a network-centric approach. After a brief presentation of measurement devices developed by the authors, their application to service monitoring platforms and QoS-driven network management design are presented. Due to space limitations, results are rather given by reference so that a holistic view can be reached.

2 QoS datasources

Monitoring systems can be categorized according to the measuring devices. In fact, KPI can be derived from active or passive probes: The first ones inject packets into the network with explicit control of timing, scheduling and sizes [8], while the second ones just capture traffic in order to analyze it in terms of protocol performance and application modeling. Active methods are used to measure delay, packet loss, jitter, available capacity and connectivity. Passive methods are useful to measure network parameters like data rate, most-used services, traffic matrix, routing, etc. and derive traffic modeling or supervise specific applications, as well as to detect fraud or hacking. Deep Packet Inspection (DPI) systems analyze traffic in detail by decoding application protocol headers; thus their exploitation allows characterizing network traffic in detail and differentiated QoS analysis can be performed. Active and passive methods can be considered complementary since they provide information about different network characteristics and parameters [9] [10].

Active probes are intrusive and overload the network with their traffic but are simple, can reproduce users behavior and may be distributed throughout the network for different tests simulating different devices (access ADSL / FTTH terminals GSM / GPRS / UMTS, etc..). A smart planning of tests, placement of probes and knowledge of the service to analyze is required to obtain a clear insight into end to end services by this means.
Passive probes are non-intrusive equipment but analyze the whole traffic in the section of network considered (access point, for instance, or a core link). Their hardware must cope with the connection bandwidth and need a great amount of computational power to analyze the data they extract. Some network elements incorporate passive monitoring facilities, such as STP (signaling transfer point) probing its own SS7 links, DWDM multiplexers or port span switches with monitoring capabilities. Thus, these deployed network elements (WDM equipment line, HLR and MSC in GSM and UMTS SGSN and GGSN in GPRS and UMTS, IP Routers, etc) provide traffic information to the network operator: The data collection is mainly done through OMCs (Operation and Maintenance Center) developed by each provider, but is sometimes reached through a mediation device. The principal drawback is that the measures provided are defined by the supplier because of lack of standardization.
Embedded agents are software pieces that can be introduced in a network element, such as a softswitch in an OLT (Optical Line Terminator), or in the customer's equipment, like a Set-Top-Box or a mobile terminal. These agents can act as active or passive probes and may be useful to monitor the perceived quality of service or QoE (Quality of Experience). Their main obvious drawback is the difficulty of deployment since they require the approval of manufacturer, service provider and end user.
In general, we can assume that an intelligent combination of probes would set up a platform for service providers, network operators and authorities to monitor traffic and supervise applications performance. Obviously, the availability of universal interfaces and standard KPI is a requirement to progress in this way.
As a first diagnosis tool, operators and big clients look after point-to-point (p2p) links, then operators and service providers watch end-to-end (e2e) connections so as to check QoS at IP layer and supervise applications performance. In the following, some examples of products designed as probes to accomplish the corresponding measurements are given.

3 P2P traffic monitoring systems

Point-to-point (p2p) measurements include throughput, latency, jitter and packet loss detected in the network layer. As it turns out, the operators have interest in supervising critical links in order to react quickly to any performance loss. One of the authors implemented a probe of high flexibility by means of a FPGA that allows generating and measuring Ethernet traffic [11] without using expensive equipment (fig. 1). Besides, the monitoring system built on them can be used to set demarcation between operator and client network.

Fig. 1. Equipments developed for Ethernet transport networks checking and operation

These are active probes normally configured in loop: The Origin device (source MAC address) sends test packets and the results are processed when they are returned. The tests are SNMP based and can be controlled by the user through a dedicated administration application that allows for specific parameters definition: Length Frame, data Rate, number of test packets, VLAN Identifier, source and destination MAC Address and test Interface. Similarly the operator can choose the type of test to execute: Single Burst Test, Continuous Burst Test or Timed Burst Test, for which the duration of the test and the time between bursts can be defined.

The user also obtains reports by means of the provided administration application: Measure, Complete and Summary Report. All of them include values of: Latency (1 µs accuracy) with maximum and medium Roundtrip value, packet loss, jitter (1 µs accuracy), maximum and medium value for each one-way and throughput.

The applications of these devices in OAM (Operations, Administration & Maintenance) systems to support IP Network and Performance Monitoring include, but are not limited to, STP (Spanning Tree Protocol) management: Regarding optical link protection issues, it is possible to set an alternative path based on real-time measurements defined by the operator as switching criteria. The whole carrier class Ethernet improvements for PTT (Packet Transport Technology) rely in devices like these ones.

Furthermore, a whole range of line cards have been added to satisfy specific customers demands and should be submitted to standardization process; for example, to monitor QoS in master-slave fashion networks (master is at the operator's domain and the slave in the customer premises) as a kind of VIP service for corporations, government and large customers. These devices are known as Ethernet Demarcation

Devices (EDD). They are gaining interest for L2- VPN and new PTT-based networks [11]. Their interfaces can be either optical or electrical. The EDD equipments developed by the authors (and tested in a public Spanish network) permit to extend optical gaps (up to 80Km) between two user switches, using the dark fiber property of the telecom operator and, allow setting alternative paths or simply determining the responsibility of eventual failures (packet loss, latency, etc.).

4 One way P2P systems measurements

To measure the IP services performance in terms of bandwidth availability and eventual differences between one way and return packet travelling, one can inject test packets and accurately timestamp the capture instant of such packets. One of the authors has developed a high-precision timestamping probe based on GPS synchronization. Its design was developed taking as a base the NetFPGA card, which provides a cost-effective, yet powerful solution with four 1-Gbps interfaces (see fig. 2).

Fig. 2. Printed board composing the core of the probe for timestamping through Global Positioning System (GPS)

The application of this system to measure OWD (One Way Delay) was presented in the CELTIC event (Paris, 2009) for a connection Madrid-Paris and has also been partially funded by the ONELAB FP7 project. The OWD measurement tool sent trains of UDP packets while other (streaming) applications were delivered e2e through the public networks. The OWD measurements are statistically analyzed in order to give an accurate mean value for the OWD. Accuracy of tens of nanoseconds is achieved by means of this simple device, which can be easily plugged in a PCI bus

in the measurement device. At the operating system, the card can be accessed through a standard socket interface, which makes it possible to analyze packet-by-packet from any user application.
On the other hand BART platform [12] (Bandwidth Available in Real Time) is an active measurement method for estimating path available capacity and other capacity-related parameters in real time over multi-domain packet-switched network paths. BART sends traffic over a network path in order to determine at which rate the path shows signs of congestion. This rate defines the path available capacity. A BART sender is transmitting IP packets at randomized inter-packet separations towards a receiver; the separation is affected by other IP traffic sharing the network path. The receiver timestamps each incoming IP packet and calculates the new inter-packet separation. The inter-packet separations at the receiver are analyzed by a Kalman filter, a statistical method for tracking not directly observable properties in real time. Combining measurements from different segments for a given end-to-end connection gives rise to a powerful tool to operate the network and find bottlenecks.

5 Service monitoring architecture

A service monitoring platform has an architecture composed by probes distributed in different segments of the network depending on its topology, the remote pre-processors, physically close to the probes, and the central repository and analyzer system (fig.3).

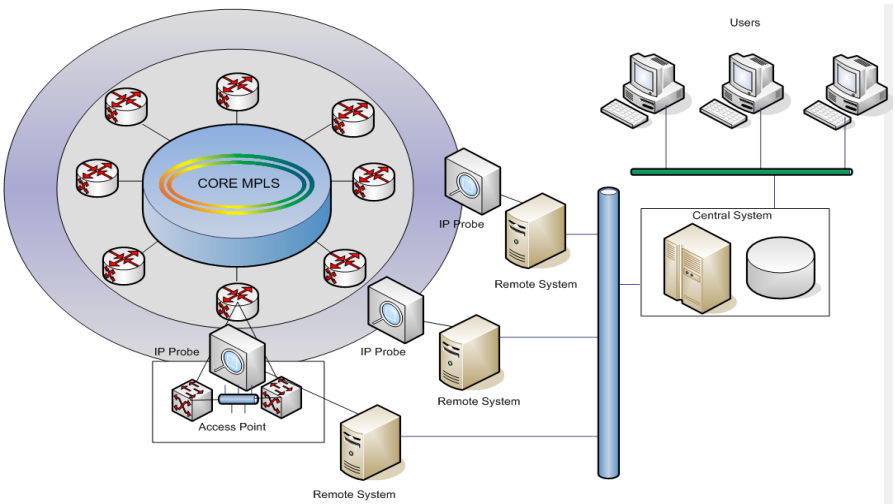

Fig. 3. Architecture of a service monitoring platform

The Remote pre-processors are able to calculate specific KPI; in fact, the captured frames are stored in these remote locations during a reasonable time in order to

analyze anomalies “post mortem”. In the central process unit, those KPI are further processed (grouped and correlated) in order to analyze the whole service platform performance and produce periodic reports for administrative and technical purposes.

Service monitoring platforms must provide capabilities for analysis, service assurance and monitoring support. Furthermore, they must support tools for diagnosing problems, such as protocol analyzers and call tracers. A wide number of functionalities must be fulfilled in order to support QoS management. These functionalities can be grouped in two areas: Traffic measures and quality measures. The first ones offer an overview of the network load (volume) and traffic characteristics along specific time periods (charged hour, cycling holiday, etc) similar to the traffic modeling mentioned above. Quality measures are targeted towards obtaining a thorough overview of how users perceive the service and how network services (offered by the operator) match service demands by applications (offered by the service providers). The traffic measures are grouped in a few parameters every hour to get a statistical estimate of the network evolution; the quality measures are taken more often (every few minutes) so that anomalies can be detected before users complain. The traffic measures cover all the protocols of the OSI tower, covering the range from level to level Liaison Implementation, and also distinguishing the particularities of each plane. As a natural nomenclature, these measures are referred to:

- Origin (probe side, close to a remote site): This range would be implicitly associated with a particular geographical area, such as a network access node.
- Destination (end opposite site towards traffic is driven): Core network elements such as application servers or control nodes.

Quality measures are obtained from statistics of failure in the protocol, number of errors in connections made and other parameters that indicate degradation in service quality.

The QoS monitoring platform (called OMEGA-Q, fig. 4) developed in Telefónica Group (Spain, Brazil, Venezuela, etc.) supports three categories of services so far: Broadband for mobile access, VoIP provision in the framework of next generation networks (NGN) and IPTV. It monitors voice-PLMN, mobile services (SMS, MMS, roaming, CAMEL…), VoIP/IMS/NGN, IPTV/MobileTV, etc. The main parameters monitored are:

- For Internet data transmission: Effectiveness of the service rate, Time to establish a connection and Loss rate information
- For VoIP quality: Effectiveness of the service rate, Call setup time
- For IPTV: Effectiveness of the service rate, Average time to swap channels and Loss of signal reception.

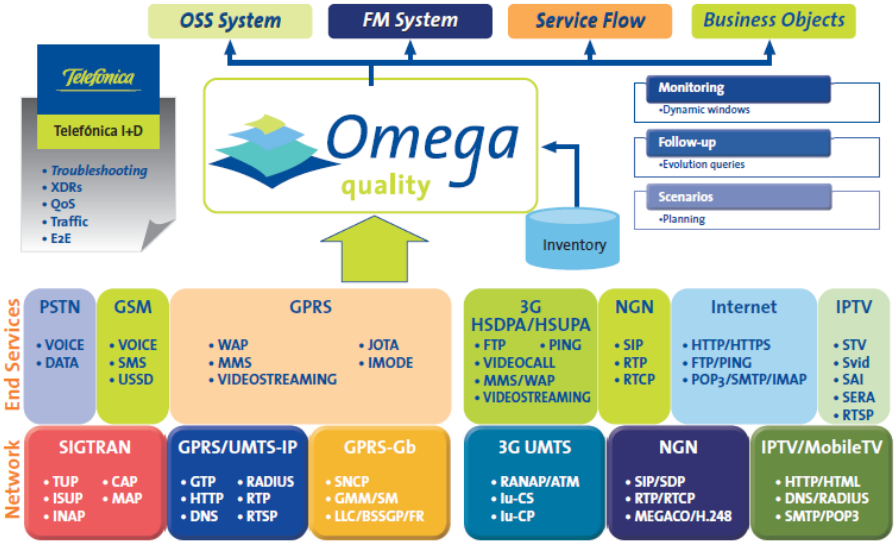

Fig. 4. Network and Services monitored by OMEGA-Q

There are several experimental initiatives for Future Internet monitoring fostered by the European Commission, each of them devoted to extend the current state of the art in different topics. See a list of referred infrastructures and traffic measurement test-beds in [10].

The European Traffic Observatory Measurement InfrastruCture (ETOMIC) was launched in 2004 to provide the scientific community with an Internet measurement platform that was fully open and reconfigurable, extremely accurate and uses GPS synchronization for timing. Now more than 20 nodes are distributed throughout Europe, with specific monitoring hardware that is integrated with the Planetlab [10] infrastructure. ETOMIC automatically performs periodic measurements that provide general network performance parameters like routes and one-way delay between all nodes of the system.

DIMES [10] uses a dedicated community of software "agents", installed by thousands of volunteers around the Globe. Using these agents, DIMES manages to measure from roughly 200 VPs on a weekly basis since 2005 and from over 350 different VPs overall since the beginning of 2009. Once installed by the user, the agent operates at a very low rate so as to have minimal impact on the machine performance and on its network connection. The project intends to explore possible relationships between the data gathered on the Internet's growth with geographical and socio- economic data, in particular for fast developing countries, to see if they can provide a measure of economic development and societal openness. The project is committed to openness and thus publishes period maps at several aggregation levels on the web. It also includes web interfaces for running remote coordinated measurements, which is used by researches around the world.

Other relevant projects are PerfSonar, a FP7 effort that serves to integrate different measurement probes in a single measurement infrastructure, and OneLab / OneLab2

IP projects that have also provided the PlanetaLab community [10] with monitoring tools.
These projects have pursued rather different objectives, and have involved a large number of research groups across Europe but most of the research groups have been involved in only one project thus being unaware of the rest.

6 QoS management and network management

Monitoring platforms link a series of precedent monitoring systems, some of them developed from previous circuit-switched network maintenance systems or ad-hoc operation platforms and management systems provided by manufacturers. Others were specifically designed and implemented for managing QoS of new services. From the point of view of pure operator, it is also interesting to obtain information from the service providers´ premises through SNMP access to extract basic statistics about network behavior. Then operators and service providers may overlap their respective platforms and integrate systems to manage QoS. This effort of integration is really important (fig. 5) in setting up Future Internet management and renders benefits to both agents since the final objective of such integration is achieving a QoS-driven network management. In practice, this approach leads to close the loop of "service provision – traffic monitoring - QoS monitoring – adaptive service provision" by means of cognitive systems acting on the network operation systems. Whether this loop requires a central operation mechanism or it is performed by autonomic agents is a further development issue although one can imagine parallel improvements following both approaches, for different scenarios, namely MANET (Mobile Ad hoc Networks), home networks, corporative virtual private networks, public networks of general purpose, etc.

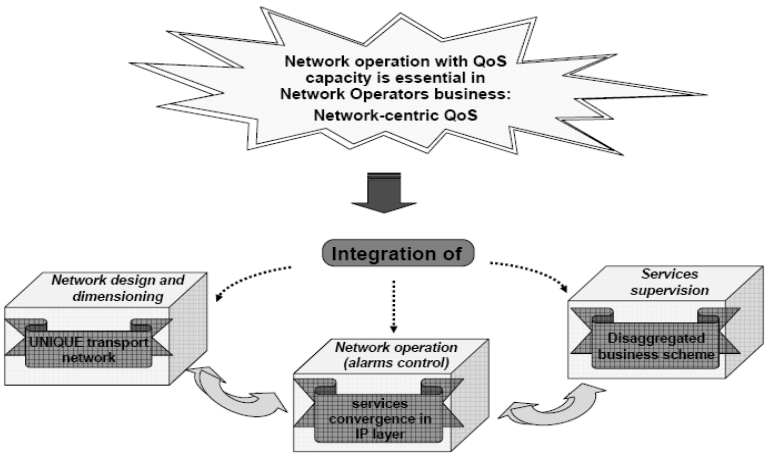

Fig. 5. Conceptual representation of a network-centric approach for QoS-driven network management architecture in future Internet

This management architecture will be able to cope with the increasing demands to offer bundled multi-services (Multi-play with IPTV/VoD/mobile), which is an important way to attract and retain customers and complies to NGN paradigms, namely convergent transport infrastructures. From a rather economic point of view, such integration is the only cost-effective solution to fulfil future Internet expectations, like operating upon virtualized resources and satisfy the "four anies", namely any access, anywhere, any time for any service users may demand.

7 Conclusions

This paper has presented several tools for service monitoring and QoS management including recently developed devices for traffic monitoring and a complete operating platform. All these elements should converge towards the objectives of extending Internet services with guaranteed quality, coping with NGN paradigms, in a cost-effective way for both service providers and network operators. Improved active and passive probes to measure traffic parameters were used to verify connectivity performance of public networks. Point-to-point measurement products were included as OAM tools for networks over packet transport technology. End-to-end measurement devices demonstrated their ability to detect network congestion and feed repositories for bottleneck analysis. Besides, an enhanced algorithm for analysis of traffic data was used to achieve traffic modeling and anomalies detection. The performance of the systems achieved is self-explained by the applications of the service monitoring world-wide deployed, as described, for IPTV, VoIP and ISP among other services.
Thus a solid base of devices, algorithms and architecture design is available for achieving network monitoring and service monitoring although other instruments, like DPI (deep packet inspection) not presented in this paper, must complete the toolbox. A further work to develop cognitive agents that perform real-time actions to correct network bottlenecks or protect it from attacks will be next step.

Acknowledgments. This work has been partially developed in the framework of the Celtic and EUREKA initiative IPNQSIS (IP Network Monitoring for Quality of Service Intelligent Support).

References

[1] A. Galis, H. Abramowicz and M. Brunner, "Management and Service-aware Networking Architectures (MANA) for Future Internet System Functions, Capabilities and Requirements", position paper in Future Internet Assembly meeting, Prague, Czech Rep., 11-13 May 2009.

[2] A. Ferreiro et al. “IP traffic monitoring for Future Internet management and governance”, pending to be published in JNSM.
[3] Cooperative Association for Internet Data Analysis (CAIDA): http://www.caida.org/home/
[4] The Traffic Monitoring and Analysis (TMA): http://www.tma-portal.eu/
[5] See, for instance the PRISM (PRIvacy-aware Secure Monitoring) project: http://www.fp7-prism.eu/
[6] A. Ferreiro et al., “Semantic Unified Access to Traffic Measurement Systems for Internet Monitoring Service”, in ICT-MobileSummit, Santander, Spain, 2009.
[7] A. Ferreiro, “Standardizing ontologies for the IP traffic measurement: A first step in QoS standardization at ETSI” in the workshop “Future Internet Design: Aspects of network monitoring, privacy and security”, Brussels, Belgium, Sept. 2009.
[8] V. Paxson, “End-to-End Internet Packet Dynamics”, in ACM SIGCOMM, , Cannes, France, Sept. 1997.
[9] T. Lindh. “A new approach to performance monitoring in IP networks combining active and passive methods”, in Proceedings of Passive and Active Measurement Workshop, Colorado, USA, Mar. 2002.
[10] FP7-MOMENT (Monitoring and Measurement in the Next Generation Technologies), http://www.fp7-moment.eu"
[11] TRAMMS (Traffic Measurements and Models in Multi-Service Networks) project measurement devices are describe in its document D4.3, (executive summary available in http://projects.celtic-initiative.org/tramms/files/TRAMMS_D4.3_ExecutiveSummary.pdf)
[12] S. Ekelin et al., ”Real-time measurement of end-to-end available bandwidth using Kalman filtering”, in proceedings to the IEEE/IFIP Network Operations and Management Symposium, Vancouver, Canada, Apr. 2006.