# QOS IN NETWORK TRAFFIC MANAGEMENT

Peter FECIĽAK, Katarína KLEINOVÁ, Jozef JANITOR
Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice,
Letná 9, 042 00 Košice, Slovak Republic, tel.: +421 55 602 7083, e-mail: {peter.fecilak, katarina.kleinova, jozef.janitor}@tuke.sk

**ABSTRACT**

*This paper deals with the optimization of data routing processes and with optimization of deployed quality of service mechanisms in computer networks. The paper addresses the problems related to requirement of monitoring and managing of network infrastructures with attention given to data routing mechanisms in network and often used QoS mechanisms. This paper also presents the concept of tool for automated network traffic management in order to network traffic optimization by identifying input curve $\alpha(t)$ and service curve $\beta(t)$ with application of mechanisms for traffic shaping and adaptive elimination of aggressive data flows. Proposed methods are experimentaly verified and compared with conventional methods.*

***Keywords:*** *quality of service, network traffic management, routing process optimization*

## 1. INTRODUCTION

Problems associated with management of network traffic are based on the sub-optimal use of network resources in currently used network technologies. Optimization of computer networks deals with the increasing performance of computer network and generally includes:

- minimize overload in the network
- minimize packet loss
- more effective usage of network resources
- minimize total delay
- maximize bandwidth (maximize number of users in used service)

By evaluation of network traffic parameters we are able to on–the–fly optimize network mechanisms that are used for routing of data or for classification and prioritization of time–critical traffic. There are two main objectives of optimization:

- operationally oriented objectives improve the quality of services in the operation of the network. These objectives include features to minimize packet loss, minimizing delays, maximizing data throughput and minimizing delay variations.
- source oriented objectives deals with effective use of network resources. Effective network management deals with monitoring of network devices to protect them against overload and due to this to packet loss and degradation of QoS in served service.

Maximization of throughput on network is key element in case of operationally oriented objectives. Network throughput can be increased by spreading the load among all the existing routes in the event of congestion at nodes. For source oriented objectives there is need for network topology discovery mechanism that can be used in automatic load–sharing. Optimization of network topology with respect to maximization of throughput and increasing of effectivity in delivery and usage of resources can be realized in the following blocks:

- analysis of network topology and the nature of the traffic
- build up transfer function which is mapped to the data flow
- identification of bottleneck in network topology
- identification of possibilities for load sharing (solution for fish–problem)
- deployment of mechanisms for classification and prioritization
- maintenance and monitoring of mechanisms deployed, or their removal

Effort in this paper is put into analysis of nature of the traffic and construction of transfer function that is mapped to traffic transmitted over network. In later sections this paper also deals with architecture of network tool and its components that acts as network maintenance and monitoring tool for traffic and routing processes optimization.

## 2. TRAFFIC NATURE AND TRANSFER FUNCTION

Distribution of load on several existing paths in communication network from the source to a destination is not appropriate in all circumstances. Experiments has shown that activation of the unequal distribution of the burden of rapid unbalanced lines at the fastest line is causing delays in service passing through the slow line. In multiaccess environment we are using pseudonode representation for communication network over which traffic is transmitted. In that case pseudonode is representing transport environment from which we are able to gather network parameters. To each pseudonode it is possible to map transfer function $\overline{F_q} = (\Gamma, \Lambda, \Psi, \Upsilon, \Theta)$, where parameters of function are as follows:

- $\Gamma$ – bandwidth (BW)
- $\Lambda$ – delay (DLY)
- $\Psi$ – delay variation (JIT)

- $\Upsilon$ – packet loss (PCKL)
- $\Theta$ – throughput of the transmission line (PCKR)

Each node in the network is dealing with routing of communication, enqueueing packets into output queues and by QoS mechanisms guarantees quality for different services [6]. Characteristic that is mapped to network node reflect queue occupation and ability of node to guarantee service curve $\beta(t)$. Transport function allows routing over each path based on weighting between parameters of transport environment. Monitoring and export of information about traffic flow plays key role in the path election mechanism and rules application for electing process of the best path (Fig. 1). When the limits of network parameters are reached in environment, it is crutial to activate potential distribution of the traffic on the lines forming loopfree path between two ends of communication.

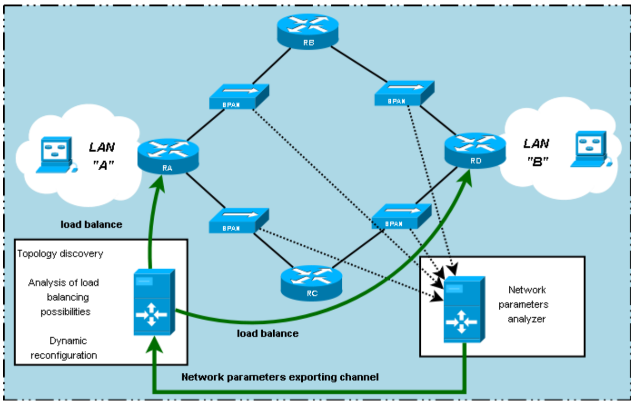
RB
SPAN
SPAN
LAN "A"
RA
RD
LAN "B"
load balance
SPAN
SPAN
Topology discovery
Analysis of load balancing possibilities
Dynamic reconfiguration
RC
load balance
Network parameters analyzer
Network parameters exporting channel

**Fig. 1** Event–driven system architecture

Compositional approach to building a computer network also allows to define the output curve of services as transfer function:

$$\beta(t) = (\beta_1 * \beta_2 * \cdots \beta_n)(t) \tag{1}$$

Proof is based on associativeness of min-plus convolution. If $y_1(t) = x_2(t)$ is the output of first node, and this output is also input for next node, then it is true that:

$$y_1(t) \geq (x_1 * \beta_1)(t) \tag{2}$$

Similarly,

$$y_n(t) \geq (x_n * \beta n)(t) \tag{3}$$

$$y_n(t) \geq ((x_{n-1} * \beta n - 1) * \beta n(t) \tag{4}$$

$$y_n(t) \geq (((x_1 * \beta 1) * \beta 2) * \cdots * \beta n)(t) \tag{5}$$

$$y_n(t) = (x_1 * (\beta 1 * \beta 2 * \cdots * \beta n))(t) \tag{6}$$

For the purpose of routing processes it is necessary to identify bottleneck in communication network and identify amount of data in transport environment. It is possible to define the amount of data in network system in time $t$ with equation:

$$v(t) = x(t) - y(t) \tag{7}$$

if $x(t)$ a $y(t)$ are representing input and output function of system. In network system $\forall t$ whose service curve is $\beta(t)$ and input curve is $\alpha(t)$ we will define the amount of data backlogged in system as:

$$v \leq \sup_{t>0}\{\alpha(t) - \beta(t)\} \tag{8}$$

Minimization of total delay is key element in QoS guarantee for time–critical services. If there is traffic flow in computer network limited by input curve $\alpha(t)$ and we are guaranteeing service curve $\beta(t)$ then maximal delay for traffic flow is defined by equation 9.

$$\delta = \sup_{t\geq 0}\{\inf_{\tau\geq 0}\{\alpha(t) \leq \beta(t+\tau)\}\} \tag{9}$$

This relationship expresses the maximum horizontal deviation of the two curves $\alpha(t)$ and $\beta(t)$. For illustration, the amount of data ($v$) backlogged in system and delay ($\delta$) is shown in figure 2.

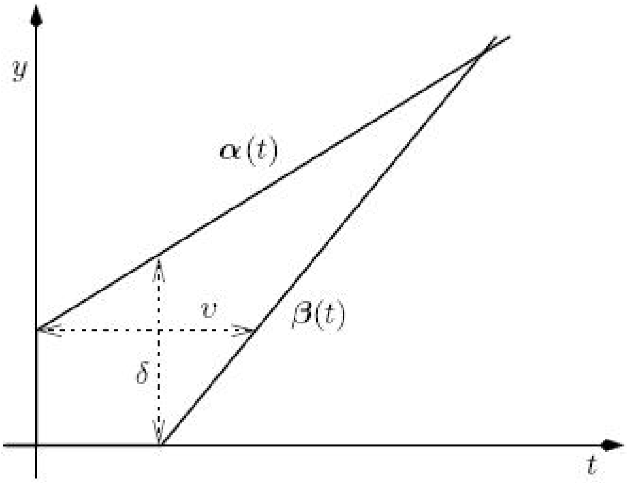

**Fig. 2** Backlog and delay in system

## 3. TRAFFIC FLOW OPTIMIZATION TOOL ARCHITECTURE

Purpose of proposed tool is to automatically reconfigure routing processes and QoS mechanisms deployed in network infrastructure with the goal of guarantee for services offerd in network. Proposed tool is using passive measurements through the measuring tool Basic Meter [1] and active measurements through SAA analyzer [2] on Cisco devices by which we are able to map network parameters of physical path to virtual network (overlay model). Proposed tool is based on following modules:

- Network traffic analyzer
- BM analyzer (ACP import)
- SAA analyzer
- Queue analyzer
- Automatic configurator
- Configuration applicator

Interconnection of modules and communication protocols that were used between modules are shown in figure 3.

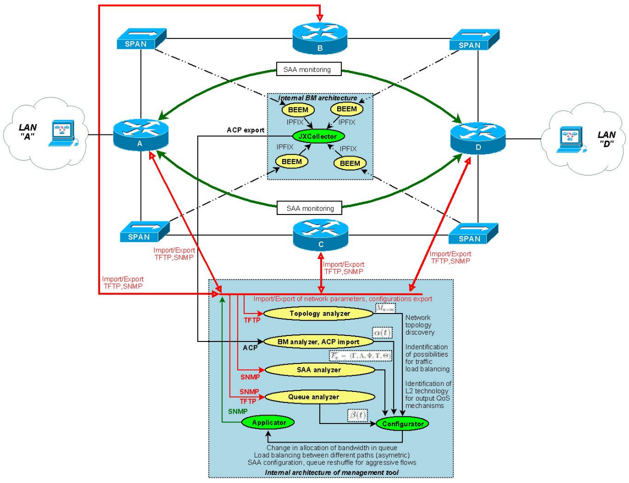
SPAN
B
SPAN
SAA monitoring
Internal BM architecture
BEEM
BEEM
IPFIX
IPFIX
JXCollector
IPFIX
IPFIX
BEEM
BEEM
LAN "A"
A
ACP export
D
LAN "D"
SAA monitoring
SPAN
C
SPAN
Import/Export TFTP,SNMP
Import/Export TFTP,SNMP
Import/Export TFTP,SNMP
Import/Export TFTP,SNMP
Import/Export of network parameters, configurations export
Topology analyzer
TFTP
$M_{n\times m}$
Network topology discovery
BM analyzer, ACP import
ACP
$\alpha(t)$
$\overline{F_q} = (\Gamma, \Lambda, \Psi, \Upsilon, \Theta)$
Indentification of possibilities for traffic load balancing
SAA analyzer
SNMP
SNMP
TFTP
Queue analyzer
Identification of L2 technology for output QoS mechanisms
SNMP
Applicator
$\beta(t)$
Configurator
Change in allocation of bandwidth in queue
Load balancing between different paths (asymetric)
SAA configuration, queue reshuffle for aggressive flows
Internal architecture of management tool

**Fig. 3** System model

### 3.1. Network topology analyzer module

Purpose of the analyzer module is to collect information about the network topology to identify opportunities for spreading the load. Building the picture of physical network topology is done by time positioning export, so each device is reporting its position in network to TFTP server by automated export of configuration and neighbors tables. CDP as data–link layer protocol was used internally for the purpose of detection of neighborship (Fig. 4).

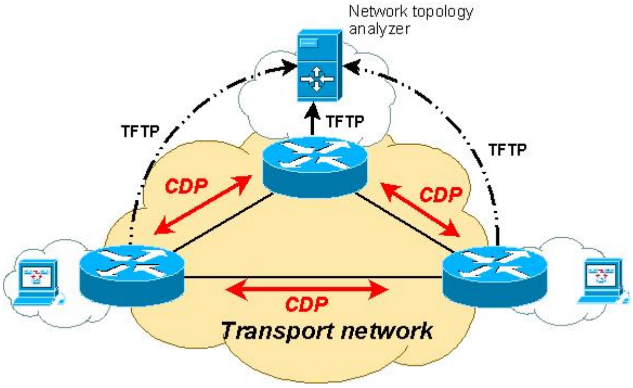

**Fig. 4** Topology detection based on CDP

### 3.2. Passive analyzer

The role of passive analyzer is to obtain the transport characteristics of the environment by non–intrusive measurements done by traffic mirroring to a specific measuring tool. Passive Analyzer must be topologically positioned so as to be able to analyze all traffic passing a transport environment. In case of the technology–limited environments, where it is not possible to implement mirroring of network traffic with analysis of data transferred to mirror analyzer, it is necessary to ensure the export of certain information with supporting protocols such as NetFlow, JFlow, NetStream.

Architecture of passive analyzer is based on (Fig. 5) [1]:

- passive probe receiving data from the monitoring line
- data collector
- analyzer and exporter

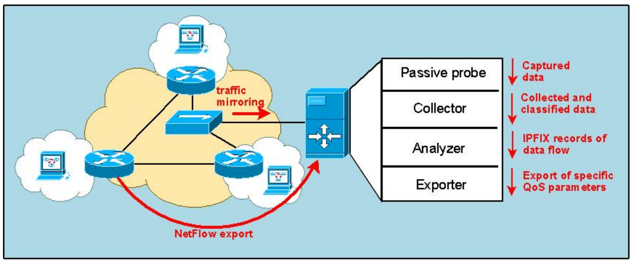
traffic mirroring
Passive probe
Collector
Analyzer
Exporter
Captured data
Collected and classified data
IPFIX records of data flow
Export of specific QoS parameters
NetFlow export

**Fig. 5** Architecture of passive measurement tool

Implementation of BM tool is trying to be close as possible to IPFIX architecture and PSAMP architecture [3]. Information model includes support for export of the NetFlow protocol versions 9. This provides an advantage over other solutions to modify export in accordance with the IPFIX since this protocol is defined as the base for its standardization. The concept of the measuring tool is designed in three layers declared by IPFIX standard. These layers include process of packets capturing, the selection of packets to their classification, export, collection, analysis and eventual archiving. Internal structure of BM tool is shown on figure 6.

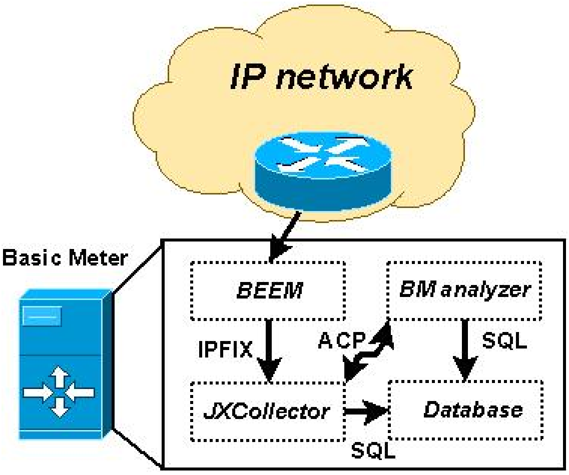

**Fig. 6** BM architecture

### 3.3. SAA analyzer and queue analyzer

The SAA analyzer is actively monitoring QoS parameters measured by SAA (IP SLA) and from the position of monitoring tool outputs are gathered in periodic intervals through the usage of SNMP protocol. Output of SAA analyzer and queue analyzer are gathered parameters:

- Number of dropped packets for each CBWFQ class
- RTT sample for each CBWFQ class
- Queue occupancy in each CBWFQ class
- Time characteristics (like delay) for collected data

### 3.4. Configurator and applicator modules

The role of configurator is the proposal of configurations or partial changes in deployed configurations for managed devices in network infrastructure and export of configurations to TFTP server. Applicator is applying configurations created by configurator module to network devices. For this purpose there are two protocols used – TFTP and SNMP. Partial configuration (changes) is loaded on TFTP server, while SNMP protocol is used as input signal to router to download configurations from the TFTP server and merge them with running configuration.

Tool for monitoring and controlling of network traffic automatically generates and applies the following initialization QoS mechanisms:

- Class-maps for single data flows
- Policy-maps for definition of QoS rules
- SAA monitoring through IP SLA

## 4. EVENT–DRIVEN AUTOCONFIGURATION

Event–driven autoconfiguration is based on the evaluation of exported parameters from passive probe, SAA gathered parameters and by monitoring of queue occupancy [4]. Purpose of event–driven autoconfiguration is to turn on load balancing mechanisms in case of overloaded queues (treshold has been reached). If the distribution of the burden continues to congestion in the queue classes and QoS policies deployed report packet loss, it is necessary to proceed to the reconfiguration of QoS mechanisms deployed. It is easy to identify most aggressive flow in regard to time stamps generated by passive probe and class in which dropping has been observed [5].

If the aggressive flow was TCP data traffic, it is automatically placed in classes with changed drop probability in which it is more probable that communication will be dropped. As TCP provides mechanism for retransmission of dropped packets it will automatically adapt to this situation and the effect will be that TCP traffic will slow down transmission. UDP communication do not support retransmission as it is unreliable connectionless oriented protocol and therefore it is not applicable to change drop probability for aggressive UDP flow. Therefore in case of UDP communication the flow is reshuffled to another class with policier defined so traffic is shaped or policed [7].

Releasing of limited resources in classes for aggressive UDP traffic or remarking classes for aggressive TCP data flows is possible only in case of free resources in different classess of priority.

## 5. EXPERIMENTAL DEPLOYMENT OF PROPOSED TOOL

The tool for network traffic management that was proposed in this paper was experimentaly deployed and its functionality was experimentaly verified. Link topology chosen for the experiments with the proposed tool is shown in figure 7. Topology is using four routers to simulate fish problem and internally there was OSPF protocol enabled with manually defined costing with the goal of balancing over different paths. There were different types of traffic generated in topology using Pagent IOS on Cisco routers.

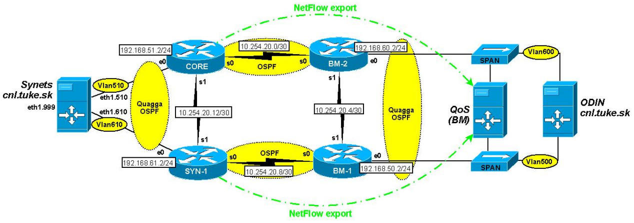

**Fig. 7** Link topology used for experiments

Experiments were related to measurement of the following parameters:

- analysis of return delay (RTT) in topology without balance
- analysis of return delay in balanced topology
- regrouping of aggressive UDP data–flow with limitation of traffic
- regrouping of aggressive TCP data–flow with change of drop probability and marking in ToS field

Experiments related to load balance were done with generation of:

- Data–flow with the power of 0 kbit/s
- Data–flow with the power of 64 kbit/s
- Data–flow with the power of 128 kbit/s
- Data–flow with the power of 150 kbit/s
- Data–flow with the power of 250 kbit/s

Transfer was carried out primarily on line with a bandwidth of 128 kbit/s and in case of the load distribution there were two lines used with capacity of 128 kbit/s and 64 kbit/s. For each of these cases the experiment was performed without balancing and with equal cost load balancing (ELB) and unequal cost load balancing (ULB). For the purpose of unequal cost load balancing there was EIGRP protocol used.

Experiments has confirmed hypotesis that load balancing is beneficial only if the amount of data in system is exceeding bandwidth of the primary line (highest bandwidth). In case that there was free bandwidth on primary line and load balancing was active between at least 2 unequal lines (128k and 64k) than delay will increase. The idea of regrouping aggressive data traffic into separate classes aimed at reducing aggressive stream has proven to be beneficial when protecting non-aggressive flows of the same QoS class against aggressive TCP or UDP flows.

## 6. CONCLUSION

This paper deals with the management of network traffic to optimize the routing process and QoS mechanisms to guarantee quality of service parameters. Particular emphasis was placed on the load balancing mechanisms in the topologies with fish problem. The effort has been devoted to monitoring of the effectiveness of deployed QoS mechanisms for automated management of network components in order to eliminate aggressive data streams. Conceptual model of automated network tool described in paper is beneficial. Proposed model of tool for dynamic reconfiguration of network components was experimentaly verified. It was proven that it is necessary to optimize routing processes or QoS mechanisms on–the–fly based on different inputs like dropping probability in QoS mechanisms, like queue occupancy or available bandwidth for spreading load across multiple paths.

## ACKNOWLEDGEMENT

This paper is the result of the project implementation: Center of Information and Communication Technologies for Knowledge Systems (ITMS project code: 26220120020) supported by the Research & Development Operational Program funded by the ERDF.

## REFERENCES

[1] GIERTL, J.: *Optimization of Measurement and Evaluation of Network Parameters in Computer Networks*, Dissertation thesis, Košice, Technical University of Košice, Faculty of Electrical Engineering and Informatics, 2006, 93 p.

[2] CISCO Systems Inc.: *Service Level Monitoring with Cisco IOS Service Assurance Agent*, [online], http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800e9012.shtml

[3] QUITTEK, J.: *Packet Sampling*, IETF HTMLl Charters [online], http://www.ietf.org/html.charters/psamp-charter.html

[4] APPENZELLER, G. – KESLASSY, I. – McKEOWN, N.: *Sizing router buffers*, SIGCOMM 2004, Portland, USA, September 2004.

[5] KOBAYASHI, H. – MARK, B. L.:*System Modeling and Analysis: Foundation of System Performance Evaluation*, Springer, March 2004.

[6] WANG, Z.: *Internet QoS Architectures and Mechanisms*, ISBN10:1558606084, 2001.

[7] WALSH, C. – DUFFIELD, N. G: *Predicting QoS Parameters for ATM Traffic Using Shape Function Estimation*, Fourteenth UK Teletraffic Symposium, Manchester, UK, March 1997.

Received August 4, 2010, accepted November 26, 2010

## BIOGRAPHIES

**Peter Feciľak** was born on 13. 07. 1983. In 2006 he graduated (MSc) with distinction at the department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at Technical University in Košice. He defended his PhD in the field of Informatics in 2009; his thesis title was "Methods of monitoring and managing of computer networks with support of QoS". Since 2010 he is working as a tutor on the Department of Computers and Informatics. His scientific research is focusing on quality of services and virtual laboratories.

**Katarína Kleinová** was born on 25. 11. 1980. In 2004 she graduated (MSc) with distinction at the department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at Technical University in Košice. She defended her PhD in the field of Computer resources and systems in 2009; her thesis title was "Solution of voice services in next generation networks". Since 2010 she is working as a tutor on the Department of Computers and Informatics. Her scientific research is focusing on quality of services and VoIP networks.

**Jozef Janitor** was born on 09. 07. 1984. In 2008 he graduated (MSc) with distinction at the department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at Technical University in Košice. Currently he is PhD student in the field of Informatics. His scientific research is focusing on VoIP networks.