ISSN 1330-3651
UDC/UDK 004.7.05:519.876

MONITORING AND MEASUREMENT OF COMPUTER NETWORK PERFORMANCE

Goran Martinovic, Bruno Petrisevac, Drago Zagar

Original scientific paper

Regardless of fast performance improvements in the field of network technologies and their pervasiveness, today's computer-demanding and service-oriented applications require efficient management of networks. Besides monitoring collision, broadcast and errors, utilization measurement of a local commutated network was carried out by means of a software tool. Measurement was carried out at two different levels of artificially generated continuous workload and by varying workload caused by intensive use of network resources. In our experiments, the monitored network showed that it is resistant to collisions and errors, but also sensitive to workload dynamics characterized by utilization changes. These changes show certain regularity and periodicity and can be considered as a good behavior pattern of a network. The approach proposed enables prediction of accessibility of computer resources by their engagement in complex distributed computer environments.

Key words: *network behavior pattern, operational analysis, performance monitoring, utilization measurement*

Nadzor i mjerenje performansi računalne mreže

Izvorni znanstveni članak

Bez obzira na brzo poboljšanje performansi mrežnih tehnologija i njihove prodornosti, današnji računalno zahtjevni i uslugama usmjereni primjenski programi, zahtijevaju učinkovito upravljanje mrežom. Uz nadzor srazova, prijenosa i pogrešaka, programskim alatom obavljeno je i mjerenje korisnosti. Mjerenje je provedeno na dvije različite razine umjetno generiranog opterećenja, te promjenjivog opterećenja izazvanog intenzivnom uporabom mrežnih resursa. U provedenim eksperimentima, nadzirana mreža pokazala je otpornost na srazove i pogreške, ali i osjetljivost na dinamičnost opterećenja, odnosno promjene korisnosti. Takve promjene pokazuju određenu pravilnost i periodnost, te se mogu smatrati dobrim uzorkom ponašanja mreže. Predloženi pristup omogućava predviđanje dostupnosti računalnih resursa pri njihovom uključivanju u složene raspodijeljene računalne okoline.

Ključne riječi: *nadzor performansi, mjerenje korisnosti, operacijska analiza, uzorak ponašanja mreže*

1 Introduction
Uvod

When we talk about computer intensive and time-critical applications, i.e. service-oriented applications and applications on demand, special attention should be paid to efficient network management. The aforementioned is additionally worsened by many users, their heterogeneity, service providers and network infrastructure [1]. As to these conditions, it is necessary to detect factors determining network performances and to have an overview of performance evaluation possibilities. According to [2], out of all network performance modeling and evaluation tools, the most complete overview of real performances as well as prediction of performance patterns can be provided by operational analysis. It can be used if network performance monitoring is enabled by corresponding software and hardware tools which yield necessary experimental results referring to the observed interval. According to [3, 4, 5], one of the important performance indicators is definitely network utilization.

Section 2 outlines most important factors determining network performance, stressing also the problem of network congestion. Section 3 describes arguments for performance evaluation, as well as tools, i.e. modeling and evaluation modes. Section 4 presents software tools for traffic generation and performance monitoring, as well as the commutator importance in design of a network. Section 5 gives an overview of two experiments in which we measured network utilization and some other performance indicators at two levels of continuous workload by additional varying workload [6]. In the same section, network performance was analyzed with reference to the performance pattern within the observed interval of 24 hours.

2 Network Performance Indicators
Pokazatelji performansi mreže

2.1 Factors affecting network performance
Čimbenici koji utječu na performanse mreže

Network communication is according to [7] limited by various factors, such as available bandwidth, network congestion, delay, server performance, and complexity of the protocol for network management. In addition to a great number of network users, there are several factors which, when combined, test usability bounds of a traditional local area network (LAN):

- Multitasking environment present in current operating systems enables concurrent network transactions.
- Intensive network applications such as the World Wide Web have also been used increasingly.
- Applications based on the client-server model do not require workstations to store information or to ensure space on the hard disk for their storage. According to [8], such applications will be probably used more significantly, but in a more sophisticated form.

According to [1, 9, 10], performance of the LAN common medium Ethernet/802.3 can be affected negatively by many factors. Ethernet uses the carrier sense multiple access/collision detect (CSMA/CD) method described in [11] and supports high transmission rates. The goal of the Ethernet is to offer the best possible delivery services and enable all devices on the common media to have equal conditions referring to data transmission. Collisions take place regularly on the Ethernet networks and can become a major problem.

2.2 Network congestion
Zagušenje mreže

A combination of powerful workstations and intensive network applications, i.e. usage of huge files, real-video, as well as demanding multimedia applications in general, requires an increasingly greater network throughput. On the other hand, the number of network users is on the rise as well. Network congestion is caused by an increase in the number of users using the network for sharing big files, access to file servers, and connection to the Internet. The consequences are increased response time, slower transmissions of files, and thereby less productive network users [12]. In order to reduce network congestion, what is necessary is either a larger bandwidth or a more effective use of the available bandwidth. Network efficiency is improved significantly by monitoring and management of its performance.

3 Performance Evaluation
Vrednovanje performansi

3.1 Need for performance evaluation
Potreba za vrednovanjem performansi

According to [2], computer architecture, operating system, database and LAN represent elements for improvement of efficiency of application execution. In case of improper use, efficiency might be reduced. Computer systems based on decentralized, parallel and distributed architectures are constantly being designed and brought into use [13]. Computer system components are becoming more complex, and at the same time requests referring to reliability and availability are higher, as in [14, 15].

3.2 Modeling tools
Alati za vrednovanje

According to [2], main types of modeling tools are analytic, simulation, testbed and operational analysis. Section 5 describes utilization measurement of a local network based on operational analysis of the existing system. Analytic modeling tools refer to a skill of describing a model by means of mathematical expressions. If the system can be considered as a set of queues by which service delivery time and waiting time may be defined analytically, then queuing analyses can be applied to problem solving. Simulation implies that a real system model is shown by means of a certain programming language for simulation execution. Simulations enable laboratory conditions for system testing without influencing the real system. Testbeds are used for studying system components and their mutual interaction in order to reach the heart of the real system. They are made of prototypes and parts of components of the real system. This method is focused on a subset of the whole systems. It might be used for the analysis of various components of networks. According to [16], compression and simplification of the system are not important in operational analysis, but rather getting information from the real system. Analysis of this information provides a good projection of future behavior, i.e. system operation. Operational analysis covers measurement and estimation of the real system. Measurements are carried out by using software and hardware monitoring devices. Hardware monitoring devices include probes and sensors, counters, as well as devices for data display and recording. Software monitoring records certain events and information about the system state. Analysis results can be used for improving performances and setting up new bounds of the system, i.e. for improvement of the existing system.

3.3 Selection criteria for modeling and evaluation tools
Kriteriji izbora alata za modeliranje i vrednovanje

As in [17], selection of a more appropriate performance evaluation method is directed by the following criteria: level of computer system development, limitation of time necessary for analysis, hardware and software tools availability, possibility of a simple and complete comparison of various methods and costs of performance analysis. Due to its advantages described in [18], Network Inspector, a software tool for network monitoring [9], is selected for utilization measurement and monitoring of the local network.

4 Testing Environment
Ispitna okolina

4.1 Network Inspector
Network inspektor

As described in [18, 23], Network Inspector is a Windows application. In combination with Fluke Networks equipment it enables network monitoring, capacity planning and error detection. The version used in this research can enable an insight into the network as well as the state of devices. It also generates network collisions, warnings and messages. Network Inspector consists of the following components:

1. **Agent Manager**, which detects and analyzes information about network and subnetworks.
2. **Microsoft Access ODBC (Open DataBase Connectivity) database**, in which the Agent stores information about network and devices.
3. **Console**, which enables the information from the selected database, as well as a general or detailed overview of this information. It is possible to select a display of the problems that have emerged, devices detected on the network and information about a particular device as well as local networks [19, 20].

Network Inspector can make the following reports: Top Interfaces by Collision Rate, Top Interfaces by Broadcast Rate, Top Interfaces by Error Rate, Top Interfaces by Average Utilization, Switch Performance, Details and Problem Log.

Utilization is, according to [2, 23], a measure of effective activity of the resources observed. A utilization diagram shows the percentage of available bandwidth used on that port. Network Inspector generates a warning if utilization crosses the warning threshold of 50 %. Also, if the error threshold is crossed (greater than 80 %), an error report is generated. Utilization in percents is calculated according to expression (1):

$$u = \left[\left(20 \cdot n_{\text{packets}}^{\text{in}} + n_{\text{packets}}^{\text{out}}\right) + \left(n_{\text{octets}}^{\text{in}} + n_{\text{octets}}^{\text{out}}\right)\right] \cdot \frac{8}{bw}, \qquad (1)$$

where:
u - utilization
$n_{\text{packets}}^{\text{in}}$ - total number of input packets
$n_{\text{packets}}^{\text{out}}$ - total number of output packets
$n_{\text{octets}}^{\text{in}}$ - number of input octets
$n_{\text{octets}}^{\text{out}}$ - number of output octets
bw - network bandwidth.

4.2 Cisco Catalyst 2950SX-24 commutator
Cisco Catalyst 2950SX-24 komutator

Cisco Catalyst 2950SX-24 described in [21] is a controlled commutator with two permanent 1000BASE-X ascending connections, which enables users' connection. It is very suitable for optical networks. Also, it is characterized by increased redundancy and availability, as well as adequate commutator connection. For the Catalyst 2950 series a Cisco Network Assistant is available, a free application for centralized management which simplifies administration tasks referring to Cisco commutators, routers and wireless access points.

5 Analysis of Experimental Results
Analiza eksperimentalnih rezultata

5.1 Experimental environment
Pokusna okolina

Measurements were carried out on a local network with 20 desktop and mobile computers and two servers networked through a commutator [21]. Computers are characterized by processors with clock frequency ranging from 1,5 to 2,8 GHz and RAM ranging from 512 MB to 2 GB, and the MS Windows XP. Servers have the same processor and capacity. All computers are networked by previously described Cisco Catalyst 2950SX-24 commutator. Network monitoring is carried out by Fluke Network Inspector, which communicates with the Cisco commutator. Traffic generator TfGen [22] generates increased workload of the commutated LAN.

Two measurements were carried out for 24 hours, as proposed in [23]. Network behavior was monitored by continuous workload of 50 % and 80 % and usual network workload. Network utilization was measured on every possible port on the commutator. In accordance with capacities of the Network Inspector tool, results are displayed for ten ports with the greatest utilization.

5.2 Experiment 1 by continuous workload
Eksperiment 1 pri stalnom opterećenju

The first measurement started at 10:00 a.m. and ended at 10:00 a.m. next day. Continuous network workload of 80 % is produced by a traffic generator TfGen, whereas additional workload is achieved by searching the Internet, data transfer, video and audio streaming, and copying 4 GB images from the server, similarly to [24].

In terms of generated and usual network traffic, the commutator enables that computers receive the data simultaneously from the preceding computer and transmit them to the next computer. For the purpose of transmission and reception of generated traffic 40 % of the bandwidth was used, which combined gives continuous network workload of 80 % at every port with speed of 100 Mbps. After one day, Network Inspector reported us about 10 ports with the greatest network utilization.

According to Fig. 1.a, great network utilization u is reached at port 22 to which the server is connected from which the network is monitored. Average utilization $\bar{u}$ was 82,38 %, while peak utilization u_{peak} was 84,26 % at 15:21 p.m. The second port was 12 (Fig. 1.b) at which $\bar{u}$ was equal to 81,65 %, and u_{peak} 84,11 % at 13:32 p.m. At port 11 (Fig. 1.c) $\bar{u}$ had the greatest value of 81,53%, and u_{peak} was equal to 84,11 % at 3:40 p.m. At port 8 (Fig. 1.d) the measured $\bar{u}$ was 81,36 % and u_{peak} was 88,61 % at 18:29 a.m. At port 21 (Fig. 1.e) $\bar{u}$ was 81,33 % while u_{peak} was 83,27 % at 12:05 a.m. On all five ports, a change in u is noticeable during the day in comparison to an approximately constant u value during the night. Within the 24 hours under observation, at those ports computers exerted network workload of 80 % and communicated successfully, ran the traffic generator, downloaded data from the Internet and the server. There follows port 15 (Fig. 1.f) at which at 9:05 p.m. $\bar{u}$ and u_{peak} were equal to 64,14 % and 83,97 %, respectively. A significant change in values of u can be noticed during the day, whereas a utilization decrease to about 40 % is noticeable between midnight and 9:00 a.m. This is caused by computer overload, and it caused failures of certain computers. Within that failure interval, the computer at port 15 was only receiving traffic from the neighboring computer connected to port 16, but it was not able to generate and transmit traffic to the computer connected to port 14, which failed. At port 18 (Fig. 1.g) at 3:55 p.m. $\bar{u}$ was measured to be 56,32 % and u_{peak} was 84,16 %. A considerable change in daytime values is noticeable, with no communication at all (i.e. u was 0) in the period between 1:00 and 9:00 a.m. Within that period, the computer at port 18 neither generated nor transmitted traffic, which means that both neighboring computers connected to ports 17 and 19 failed. At port 16 (Fig. 1.h) at 1:10 p.m. $\bar{u}$ and u_{peak} were 56,07 % and 86,98 %, respectively. An expected utilization change in daytime values is noticeable, but between 6:00 p.m. and 9:00 a.m. u was about 40 %. During that period the computer was only transmitting traffic to the next computer at port 15, but it did not receive any traffic from the preceding computer at port 9, which was out of order. There follows port 10 (Fig. 1.i) at which at 10:47 a.m. the measured $\bar{u}$ and u_{peak} were 56,02 % and 87,31 %, respectively. A significant change in daytime values is noticeable, and a decrease of u to about 40 % between 6:00 and 9:00 a.m. During that time, the computer at port 10 was only receiving traffic from the computer at port 11, but it could neither generate nor transmit traffic since the neighboring computer at port 9 failed. Finally, at port 24 (Fig. 1.j) at 9:12 a.m. $\bar{u}$ and u_{peak} were 50,86 % and 84,43 %, respectively. A significant change of u is noticeable by 3:00 p.m., and after that by 9:00 a.m. u was about 40 %. After that, the computer did not receive traffic from port 17, which failed, but it only transmitted traffic to port 22.

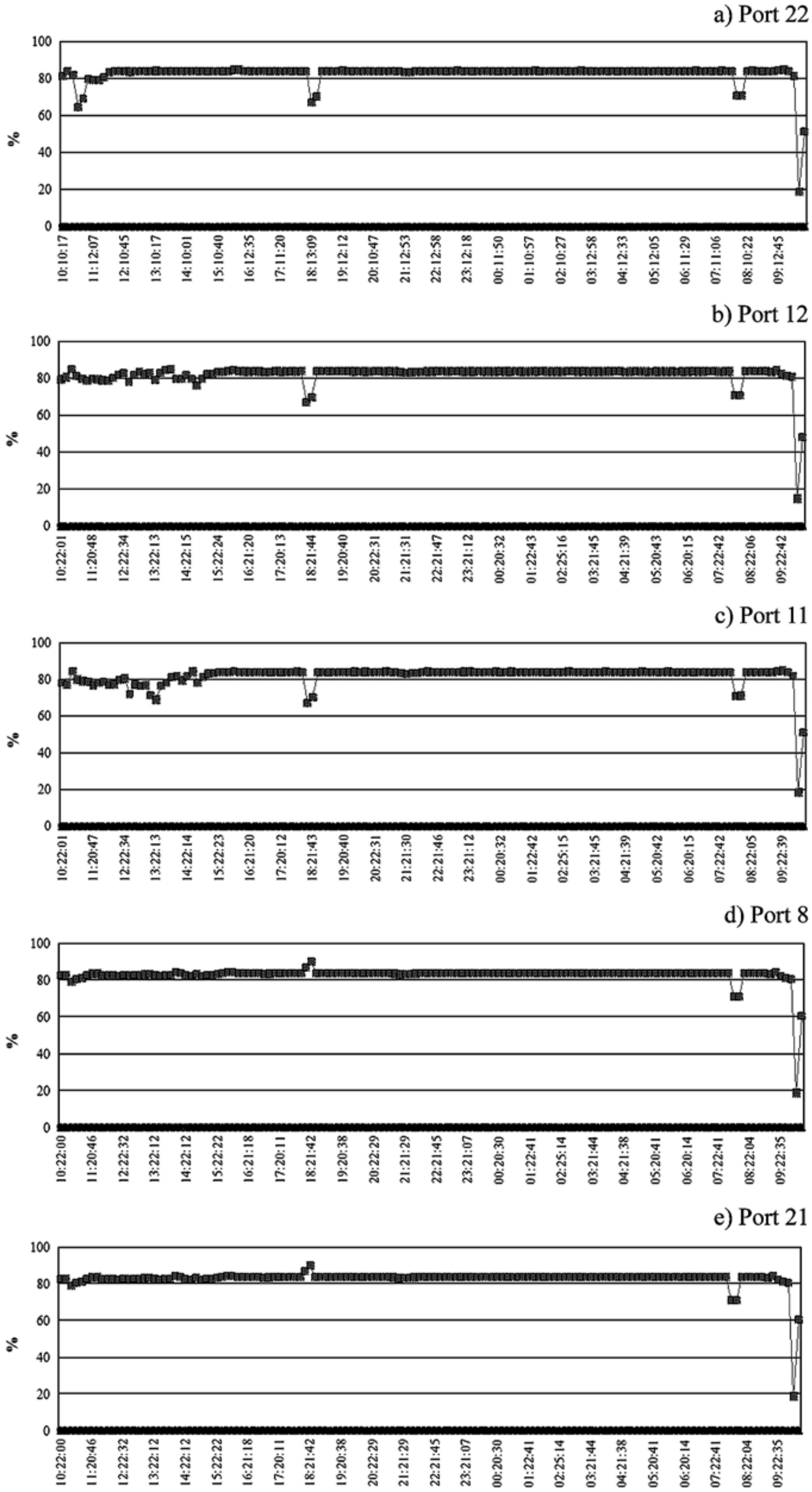

Figure 1.a-e *Utilization at first 5 ports with the greatest utilization in Experiment 1*
Slika 1.a-e. *Korisnost na prvih 5 pristupa prema razini korisnosti u Eksperimentu 1*

Tab. 1 shows $\bar{u}$ and u_{peak} at every port for Experiment 1, as proposed in [19]. The total average network utilization $\bar{u}_{total}$ at these ten ports is 71,20 %. The standard deviation σ_u is 12,88 %, because of the range of single $\bar{u}$ (at ports) from the highest 82,38 % to the lowest u_{low} 50,86 %.

Fig. 2 shows values $\bar{u}$, u_{peak} and $\bar{u}_{total}$ for Experiment 1. The greatest positive deviation from the total average value is present at port 22 (+13,14 %), whereas port 24 records the greatest negative offset of –20,34 %.

Computers at ports with measured values $\bar{u}$ that are greater than $\bar{u}_{total}$ have successfully completed their testing jobs, achieving $\bar{u}$ between 80 and 85 %. Computers connected to ports at which individual measured values of $\bar{u}$ are less than $\bar{u}_{total}$ did not meet the mentioned values of $\bar{u}$, due to failures of computers they communicated with because of higher workload. Peak utilizations u_{peak} are equal at almost all ports, with the exception of port 8 with u_{peak} of

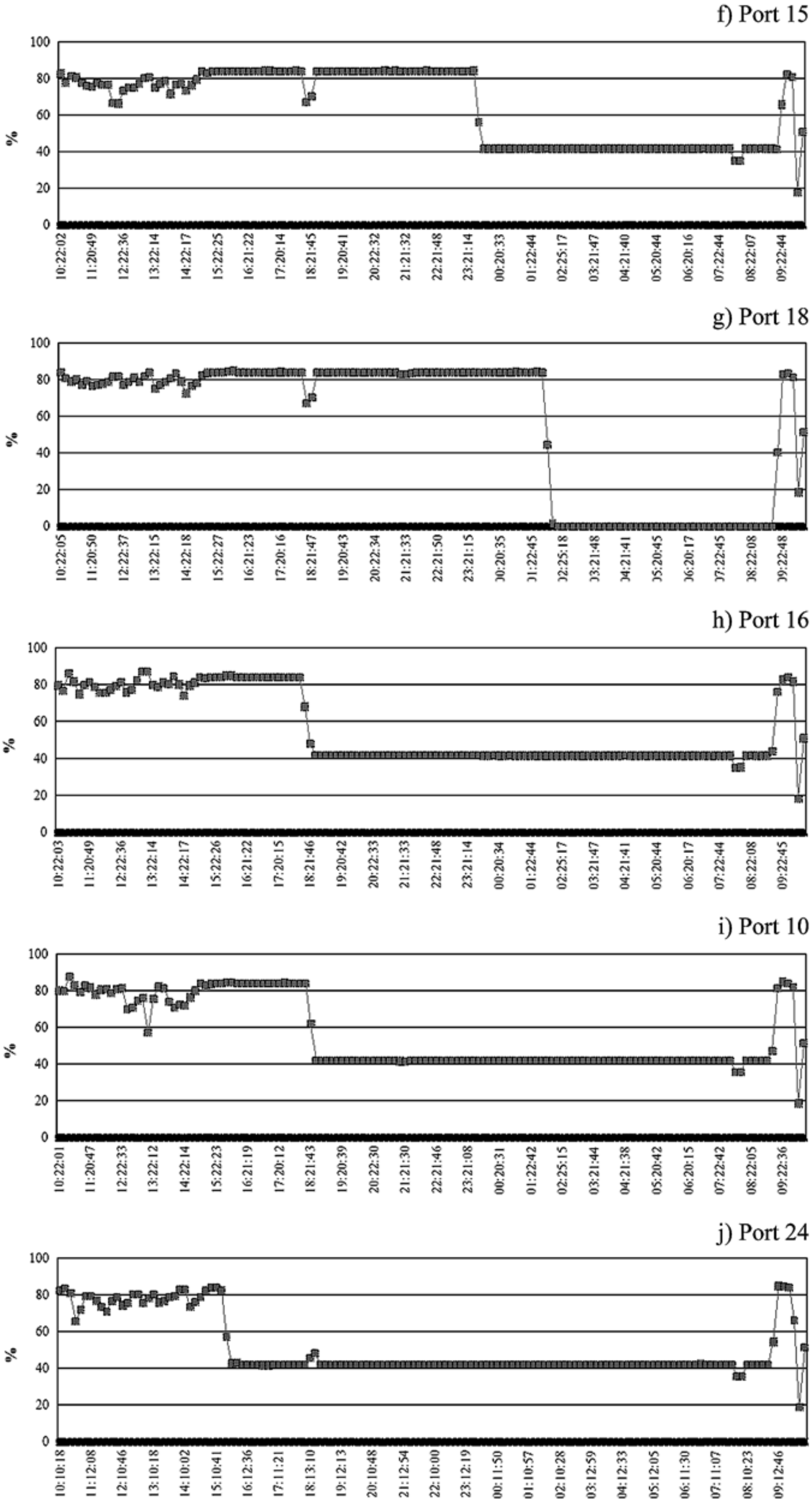

Figure 1.f-j *Utilization at second 5 ports with the greatest utilization in Experiment 1*
Slika 1.f-j. *Korisnost na drugih 5 pristupa prema razini korisnosti u Eksperimentu 1*

88,61 %. There was no network congestion during the experiment.

5.3 Experiment 2 by varying workload
Eksperiment 2 pri promjenjivom opterećenju

The second measurement started at 1:30 p.m. and ended at 1:30 p.m. next day. Similarly to [25], continuous network workload of 50 % is achieved by means of a traffic generator TfGen, whereas additional workload is achieved by searching the Internet, data transfer, video and audio streaming, and copying 2 GB images from the server.

Artificially generated traffic was carried out pairwise. By means of a traffic generator and through the commutator, every computer received the data simultaneously from the computer it was paired to and transmitted the data to the

Table 1 *Network utilizations in Experiment 1*
Tablica 1. *Korisnost mreže u Eksperimentu 1*

Port	$\bar{u}$/%	u_{peak}/%	$\bar{u}_{total}$/%	σ_u/%
22	82,38	84,26	71,20	12,88
12	81,65	84,21		
11	81,53	84,11		
8	81,36	88,61		
21	81,33	83,27		
15	64,14	83,97		
18	56,32	84,16		
16	56,07	86,98		
10	56,02	87,31		
24	50,86	84,43		

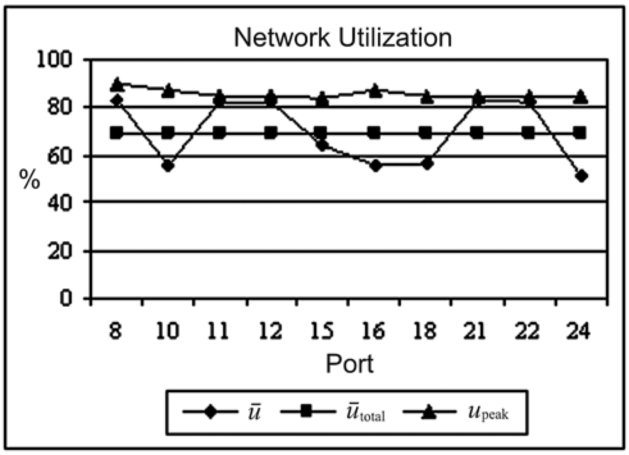

Figure 2 *Network utilization for Experiment 1*
Slika 2. *Korisnost mreže za Eksperiment 1*

same computer. For the purpose of reception and transmission of generated traffic 25 % of the bandwidth was used, which combined gives continuous network workload of 50 % at every port with the speed of 100 Mbps. After 24 hours Network Inspector recorded 10 ports with the greatest network utilization.

The greatest network utilization is reached at port 7 (Fig. 3.a) to which the server is connected at which the antivirus software is replenished and from which a 2 GB image was copied to other computers. The second server connected to port 8 generated traffic by means of a TfGen which exerted continuous network workload of 50 % at port 7. At 2:20 p.m. the values of $\bar{u}$ and u_{peak} were 58,27 % and 95,21 %, respectively. A noticeable high value of u is observed during daytime due to jobs executed by this server, and more uniform values of about 50 % during night.

Network utilization at port 7 usually crossed 80 %, and that is the value at which Network Inspector reports an error (▲). When the utilization value is 50 %, a warning (•) is reported. These messages are recorded in Problem Log and they indicated that the network administrator should react and prevent possible network congestion. Measurement equipment listed problems containing error messages due to network utilization greater than 80 % at port 7, as well as warning messages due to network utilization greater than 50 % at other ports.

The second is port 8 (Fig. 3.b) to which the server is connected from which network monitoring is carried out and which generated and transmitted traffic to the server with antivirus software at port 7. At 1:01 a.m. the value of $\bar{u}$ was 52 %, and of u_{peak} 55,96 %. At port 22 (Fig. 3.c) at 1:01 p.m., $\bar{u}$ and u_{peak} were 51,67 % and 61,32 %, respectively. The value of u was greater during daytime and continuous during night, but its value decreased to about 25 % between 9:00 and 10:00 a.m. During that period the computer at port 22 was only transmitting data to the computer connected to port 24, but it did not receive any traffic from it. At 12:40 p.m., at port 15 (Fig. 3.d) the values of $\bar{u}$ and u_{peak} were 51,51 % and 62,73 %, respectively. At 4:31 p.m. at port 16 (Fig. 3.e) $\bar{u}$ and u_{peak} were 51,42 % and 63,04 %, respectively. A significant change of u is noticeable during daytime, primarily because of copying images from the server. Then it is continuous during the night, after which it fails to communicate between 9:00 and 10:00 a.m. In that period, computers neither mutually transmitted nor received data at ports 15 and 16. At 00:11 a.m., at port 24 (Fig. 3.f) $\bar{u}$ and u_{peak} were 51,25 % and 56,40 %, respectively. A slight difference of u is noticeable during daytime, continuous u is recorded during the night, but between 9:00 and 10:00 a.m. u is reduced to about 25 %. Within that one hour the computer at this port did not generate traffic, but it only received traffic from the computer at port 22 it was in pair with. At 12:12 p.m., at port 21 (Fig. 3.g) $\bar{u}$ and u_{peak} were measured 43,08 % and 61,23 %, respectively. The change of u during daytime was expected, but between 1:00 and 10:00 a.m. it was reduced to about 25 %, which caused failure as to traffic generation. At 1:21 p.m., at port 17 (Fig. 3.h) $\bar{u}$ and u_{peak} were 43,05 % and 60,52 %, respectively. The u changed during daytime and decreased to about 25 % between 1:00 and 10:00 a.m. During that period, the computer at port 17 generated and transmitted traffic to the computer connected to port 21, but it did not receive any traffic from it. At 12:20 p.m., at port 19 (Fig. 3.i) $\bar{u}$ and u_{peak} were measured 41,82 % and 61,11 %, respectively. A change of u is recorded in daytime, which is then reduced to about 25 % between 1:00 and 9:00 a.m., after which there is no traffic flow between 9:00 and 10:00 a.m. As of 1:00 a.m. the computer at port 19 did not receive, but it only generated and transmitted traffic to the computer at port 18. Between 9:00 and 10:00 a.m. computers failed at ports 18 and 19, which caused a break in traffic transmission and reception. At 12:40 p.m., at port 18 (Fig. 3.j) $\bar{u}$ and u_{peak} were 41,69 % and 62,09 %, respectively. The corresponding utilization diagram is similar to the previous one, since these computers operated in pairs. A change of u is noticed during daytime, utilization is reduced to about 25 % between 1:00 and 9:00 a.m., when the computer at port 18 stopped generating traffic and only received traffic from the computer at port 19. Between 9:00 and 10:00 a.m. both reception and transmission were stopped because of the failure of computers at ports 18 and 19.

Tab. 2 shows measurement results referring to network utilization in Experiment 2 for ten ports with the greatest values of $\bar{u}$, u_{peak} and $\bar{u}_{total}$, which amounts to 48,57 % at these ten ports, whereas standard deviation σ_u is equal to 5,71 %. Individual average utilizations at ports range between the highest 58,27 % and the lowest 41,69 %.

Fig. 4 shows a network utilization diagram for ten ports with the highest measured values in Experiment 2.

The greatest positive offset from the total average value at port 7 is +9,70 %, while at port 18 the greatest negative offset of $\bar{u}_{total}$ was –6,88 %. At six ports individual $\bar{u}$ are greater than $\bar{u}_{total}$. Computers at these ports did their job with minor failures and $\bar{u}$ greater than 50 %. Computers connected to ports at which individually measured $\bar{u}$ are less than $\bar{u}_{total}$ did not reach the expected $\bar{u}$ of 50 %. The reason for that are computer failures in specific periods of

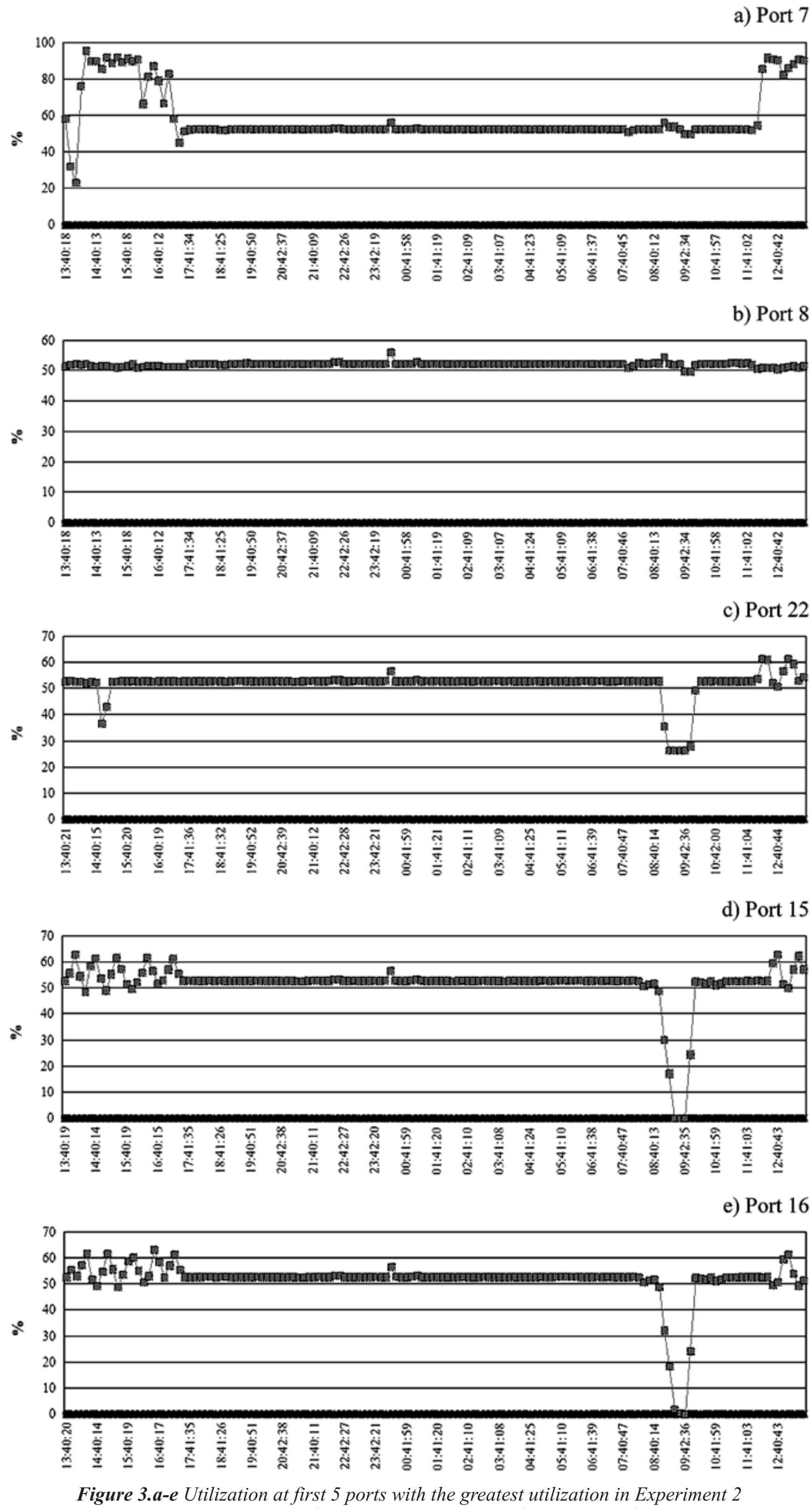

Figure 3.a-e *Utilization at first 5 ports with the greatest utilization in Experiment 2*
Slika 3.a-e. *Korisnost na prvih 5 pristupa prema razini korisnosti u Eksperimentu 2*

time, i.e. a break in data generation and transmission due to high workload. Values of u_{peak} are almost equal at all ports, excluding port 7 at which the antivirus software server is placed, so that the greatest u_{peak} of 95,21 % was measured exactly at it. No network congestion was recorded during measurements.

Network utilization measurements at generated constant workload of 80 % in Experiment 1 and 50 % in Experiment 2 resulted in average utilization values $\bar{u}$ of 69,44 %, i.e. 48,57 %. In both experiments no congestion of the commutated network was recorded, and neither were collisions and errors, but values of $\bar{u}$ were lower than expected, mostly due to failures of particular computers, but partly because of insufficient processor capacity for the given working conditions. Accuracy of network parameters measurement is described in [26] and [27].

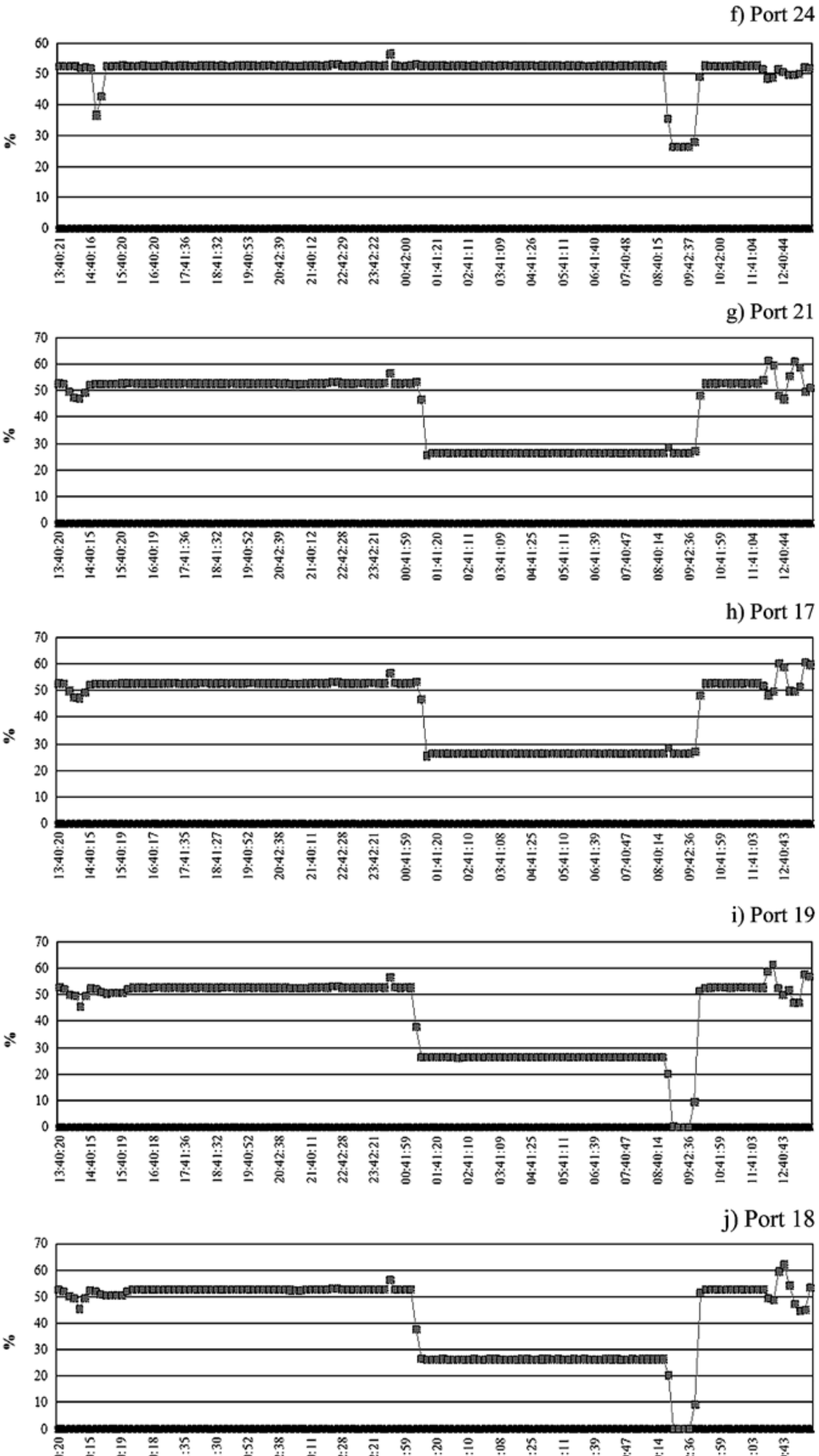

Figure 3.f-j *Utilization at second 5 ports with the greatest utilization in Experiment 2*
Slika 3.f-j. *Korisnost na drugih 5 pristupa prema razini korisnosti u Eksperimentu 2*

6 Conclusion
Zaključak

Pervasive and rapid development of network technologies and computer systems needs precise performance monitoring, evaluation and control. This also implies not only active network monitoring and management by the administrator, but also a series of procedures related to autonomous network management possibly supported by hardware and software components. That management was executed at operational, information, communication and functional level. Operational analysis provides the best insight into network performance. Local commutated network utilization and other performance indicators were measured. Network utilization and other parameters were measured in duration of 24 hours through two experiments. Workload was generated by the traffic generator made by means of software. In the first and the second experiment continuous

***Table 2** Utilization in Experiment 2*
***Tablica 2.** Korisnost u eksperimentu 2*

Port	$\bar{u}$/%	u_{peak}/%	$\bar{u}_{total}$/%	σ_u/%
7	58,27	95,21	48,57	5,71
8	52,00	55,96		
22	51,66	61,32		
15	51,51	62,73		
16	51,42	63,04		
24	51,25	56,40		
21	43,08	61,23		
17	43,04	60,52		
19	41,82	61,11		
18	41,69	62,09		

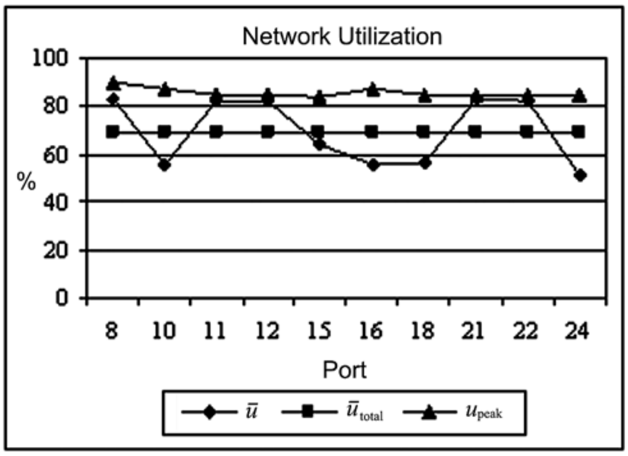

***Figure 4** Utilization for Experiment 2*
***Slika 4.** Korisnost mreže za Eksperiment 2*

workload was 80 % and 50 %, respectively. In addition to that continuous workload, varying workload consisted of various data transfers from the local server and the Internet.

By observing performance indicators we concluded that the commutated network is not liable to errors, congestion and collision. Utilization at monitored ports indicates a possibility for determination of a utilization, performance and network capacity behavior patterns. For a more complete insight into network performance pattern, it is necessary to carry out measurements in a longer period of time and observe seasonal changes. Network parameter patterns provide important information which can initiate engagement of additional capacities of the observed network segment. In other words, intervals in which the network is overloaded even without additional workload (low utilization) are proposed and no high performance is to be expected from it. Current and further research deals with higher network complexity, heterogeneity and dynamics. It is targeted to inclusion of non-dedicated computers and wireless network resources in computational clusters and grid infrastructure.

8 Acknowledgement
Zahvala

This work was supported by research project grant No. 165-0362980-2002 from the Ministry of Science, Education and Sports of the Republic of Croatia.

9 References
Literatura

[1] Guoqiang, M.; Habibi, D. Loss Performance Analysis for Heterogeneous on-off Sources with Application to Connection Admission Control. // IEEE/ACM Transactions on Networking, 10, 1(2002), 125-138.
[2] Fortier, P. J.; Michel, H. E. Computer Systems Performance Evaluation and Prediction, Digital Press, USA, 2003.
[3] Green, K. Internet Game Network Utilization on College Campuses. // Journal of Computing Sciences in Colleges, 20, 5(2005), Consortium for Computing Sciences in Colleges, 126-127.
[4] Shiomoto, K.; Chaki, S.; Yamanaka, N. A Simple Bandwidth Management Strategy Based on Measurements of Instantaneous Virtual Path Utilization in ATM Networks. // IEEE/ACM Transactions on Networking, 6, 5(1998), 625-634.
[5] Weiguang, S.; MacGregor, M. H.; Gburzynski, P. Load Balancing for Parallel Forwarding. // IEEE/ACM Transactions on Networking, 13, 4(2005), 790-801.
[6] el Allali, H.; Heijenk, G.; Lo, A.; Niemegeers, I. A Measurement-Based Admission Control Algorithm for Resource Management in Diffserv IP Networks. // in Proc. of IEEE 17th Int. Symp. Personal, Indoor and Mobile Radio Communications, 2006., 1-5.
[7] Parthasarathy, M. Analysis of Network Management of Remote Network Elements, in Proc. of Int. Conf. on Networking, Systems and Mobile Communications and Learning Technologies, 2006., pp. 57.
[8] Nieh, J.; Yang, S. J.; Novik, N.Measuring Thin-Client Performance Using Slow-Motion Benchmarking. // ACM Transactions on Computer Systems, 21, 1(2003), 87-115.
[9] Breitbart, Y.; Chee-Yong, C.; Garofalakis, M.; Rastogi, R.; Silberschatz, A. Efficiently Monitoring Bandwidth and Latency in IP Networks. // in Proc. 20th Annual Joint Conf. of the IEEE Computer and Communications Societies, 2001., pp. 933-942.
[10] Li, M.; Sandrasegaran, K. Network Management Challenges for Next Generation Networks. // in Proc. of 30th Annual IEEE Conference on Local Computer Networks, 2005., 593-598.
[11] Harfoush, K.; Bestavros, A.; Byers, J. Measuring Bottleneck Bandwidth of Targeted Path Segments. // in Proc. of 22nd IEEE Annual Joint Conf. of the Computer and Communications Societies, 2003., pp. 2079-2089.
[12] Zhao, Yong-xiang; Li, Chun-xi; Chen, Chang-jia. Sandwich: a New Tool That Can Identify Bottleneck Link by End to End Measurement. // in Proc. of Int. Conf. on Communication Technology, 2006., pp. 1-4.
[13] Lowekamp, B. B. Combining Active and Passive Network Measurements to Build Scalable Monitoring Systems on the Grid, ACM SIGMETRICS Performance Evaluation Review, 30, 4(2003), pp. 19-26.
[14] Egyhazy, M. W.; Yao, L. Predicted Sum: A Robust Measurement-Based Admission Control with Online Traffic Prediction. // IEEE Communications Letters, 11, 2(2007), 204-206.
[15] Jain, M.; Dovrolis, C. End-to-End Available Bandwidth: Measurement Methodology, Dynamics, and Relation with TCP Throughput. // IEEE/ACM Transactions on Networking, 11, 4(2003), 537-549.
[16] Papagiannaki, K.; Cruz, R.; Diot, C. Characterization: Network Performance Monitoring at Small Time Scales. // in Proc. of 3rd ACM SIGCOMM Conf. on Internet Measurement, 2003., pp. 295-300.
[17] Montes, M.; Swiatczak, J.; Lesniewski, P. J.; Thomas, J. C.; Golczak, M. Universal Laboratory Networking System (ULabNet). // in Proc. of IEEE Instrumentation and Measurement Technology Conf., 2006., pp. 986-991.
[18] Fluke Networks, www.flukenetworks.com.

[19] Hanemann, A.; Jeliazkov, V.; Kvittem, O.; Marta, L.; Metzger, J.; Velimirovic, I. Complementary Visualization of perfSONAR Network Performance Measurements. // in Proc. of 2006 Int. Conf. Internet Surveillance and Protection, 2006., pp. 6-6.
[20] Habib, A.; Fahmy, S.; Bhargava, B. Monitoring and Controlling QoS Network Domains. // Int. Journal of Network Management, 15, 1(2005), 11-29.
[21] Cisco Systems, Inc., www.cisco.com.
[22] Traffic Generator, TfGen, www.st.rim.or.jp/~yumo/pub/tfgen.html.
[23] Martinovic, G.; Zagar, D.; Tomic, D. Network performance monitoring and utilization measurement. // in Proceedings of the European Computing Conference, Vol. 1, Lecture Notes in Electrical Engineering Vol. 27 (N. Mastorakis, V. Mladenov, V. Kontargyri, Eds.), Springer, New York, 2009., pp. 601-606.
[24] Bergeron, R. J. Measurement of a Scientific Workload Using the IBM Hardware Performance Monitor. // in Proc. 1998 ACM/IEEE Conference on Supercomputing, 1998., pp. 49.
[25] Raz, D. Efficient Network and Traffic Monitoring. // in Proc. 10th IEEE/IFIP Symposium on Network Operations and Management Symposium, 2006., pp. 587-587.
[26] Roughan, M. Fundamental Bounds on the Accuracy of Network Performance Measurements, ACM SIGMETRICS Performance Evaluation Review. // 33, Issue 1, ACM Press, 2005., pp. 253-264.
[27] Saito, H.; Chusho, T. Design and Implementation of a Network Performance Evaluation System through Client Observation. // in Proc. of 10th Annual Internet Society Conference, http://www.isoc.org/inet2000/dproceedings/longtoc.htm, 2000.

Authors' Address
Adrese autora

Associate Professor Goran Martinovic, PhD
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia
Phone: +385 31 224 766
Fax: +385 31 224 605
e-mail: goran.martinovic@etfos.hr

Bruno Petrisevac, BSc
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia

Full Professor Drago Zagar, PhD
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia