Monitoring and Optimization in computer networks services at Faculty of Electrical Engineering UGM

Mohammad Fal Sadikin

Lecturer in STMIK Amikom Yogyakarta

Abstract

Due to the large number of user at Faculty of Electrical Engineering Gadjah Mada University, the quality of computer networks services decrease not only in local networks but also in internet networks, such as low quality network connection, failure connection frequently occurs, unsatisfactory application run in the networks system, high latency operation, etc. Therefore, Optimization is one of the ways to solve this problem to increase performance and provide better services.

Both monitoring and scanning in networks services are used as method to identify the problems and try to solve the problems in order to optimize the networks services. The monitoring is held in a month particularly within the most crowd traffic period in several gateway posts and several main VLANs with network tapping method.

From the monitoring and scanning show that in order to optimize the networks services; several networks systems must be reformulated, such as access control list, optimization of proxy system, and redesign network traffic to fulfill the optimization objective.

Keywords: Network Monitoring, Optimization, Network Management.

1. Introduction

Currently, Electrical Engineering UGM has good enough networks infrastructure, which serve the necessary of network connection and any applications which is run in the network services.

The devices technology and security system are also good enough with firewall system, proxy system, and several good devices and application technology which support the system services.

However, the system is still unsatisfactory in performance, such as unsatisfactory in serve connection and serve the applications run above the system, high latency operation, etc. these are indicated by the large number of users who often complain with the systems performance, such as low quality networks connection especially at the most crowd traffic in working hour within 08.00am – 4.00pm. Therefore the systems need optimization to increase the quality of services as well as the system technology.

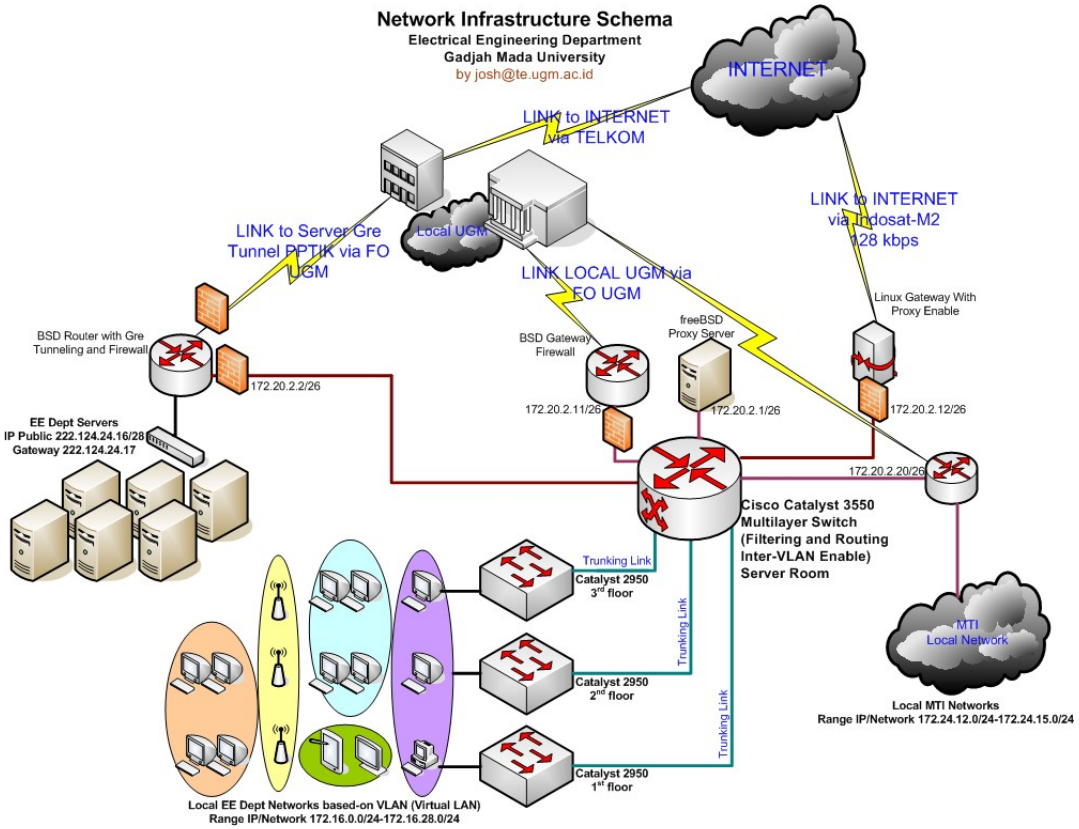

Figure 1: Network Infrastucture Scheme TE UGM (pictured by Josh).

Monitoring and scanning method are the way to identify the problems and try to solve the problem in order to optimize the systems. The detail about method, the results of monitoring and scanning, and the problem solution will be investigated in this paper.

2. Objectives

The main objectives of this project are listed as follows.

1. To identify the problems of the system and try to solve the problems in order to optimize the system performance.

2. To obtain the references of user's pattern to identify users needs to be able to redesign the system as well as users necessary to optimize the system.

3. To obtain references to evaluate and redesign the security system as well as users pattern.
4. To obtain references to redesign network management as well as the project results.
5. To obtain references to formulize network policy for achieving a good performance and a system's security goals.

3. Methods

Several monitoring with several protocol analyzers such as wireshark, iris, etc. are held to obtain data of traffic with network tap method. Network tap is a method to obtain a way to access data flowing across a computer network.

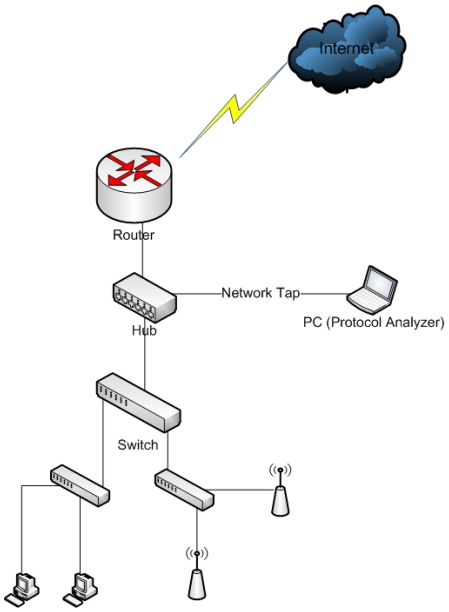

Figure 2: Network Tap.

The networks taps are made with several rules are listed as follows.

1. The main monitoring is held at network gateway to obtain the main data of traffic which go in and out Electrical Engineering UGM network systems.
2. Monitoring is also held in two main proxies (MTI proxy and T.E. Proxy) in the networks system.
3. Several monitoring are also held in several important Vlans to obtain pattern of users in the networks system.
4. Each monitoring point is held within a full month to obtain better data.

4. Monitoring results and Problem solution

4.1. Gateway T.E. UGM

4.1.1. Monitoring results of Gateway T.E. UGM

Gateway T.E. UGM is a main traffic to local connection UGM networks, such as traffic from T.E. UGM to other faculty in UGM environment. From monitoring results, gateway destination is showed as following table.

Date	Time	10.13.253.25	172.20.2.14	10.13.254.101	Others
2 June 2008	10.00	65,05%	32,28%	1,40%	1,27%
4 June 2008	09.00	60,43%	36,09%	1,93%	1,55%
6 June 2008	09.00	66,33%	30,63%	1,62%	1,42%
9 June 2008	11.00	57,23%	35,12%	3,61%	4,04%
12June 2008	13.00	59,39%	35,58%	2,20%	2,83%

Figure 3: Gateway Destination

The table gateway destination from figure 3 shows that the traffic destinations mostly connect to the three local servers UGM, which are server to storage entertainment files which are dedicated for student entertainment needs. The students usually upload and download huge entertainment files such as video or audio file. It is legal activity but definitely, it is not a good time for entertainment activity especially within working hour and can decrease the effective of learning activity because many students do not concentrate with learning and working activity and more focus to entertainment activity. Moreover, it can cause the crowd traffic and disturb the traffic stability. Therefore the accessible of the server must be restricted within working hour and set to be normal again in outside of working hour. The table shows that the three upper IP are.

1. 10.13.253.25 = (65,05%), UGM Local Server
2. 172.20.2.14 = (32, 28%) FTP TE Server
3. 10.13.254.101 = (1, 40%) UGM Local Server

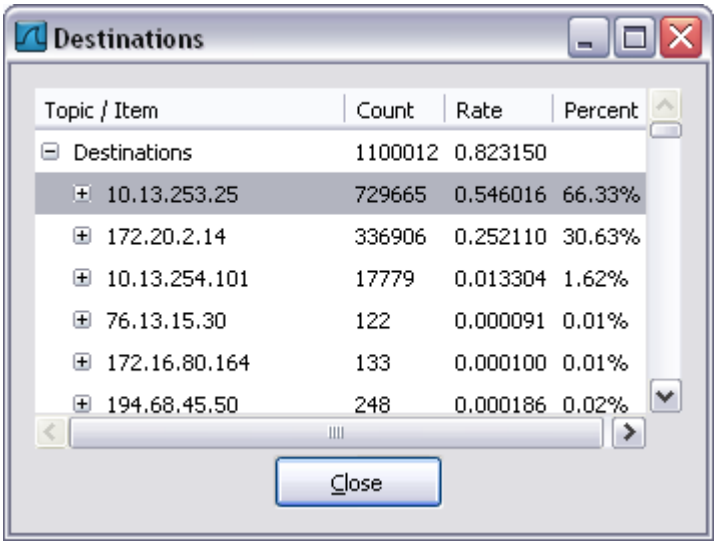

Figure 4: Sample of Gateway Destination (2 June 2008, 10.00)

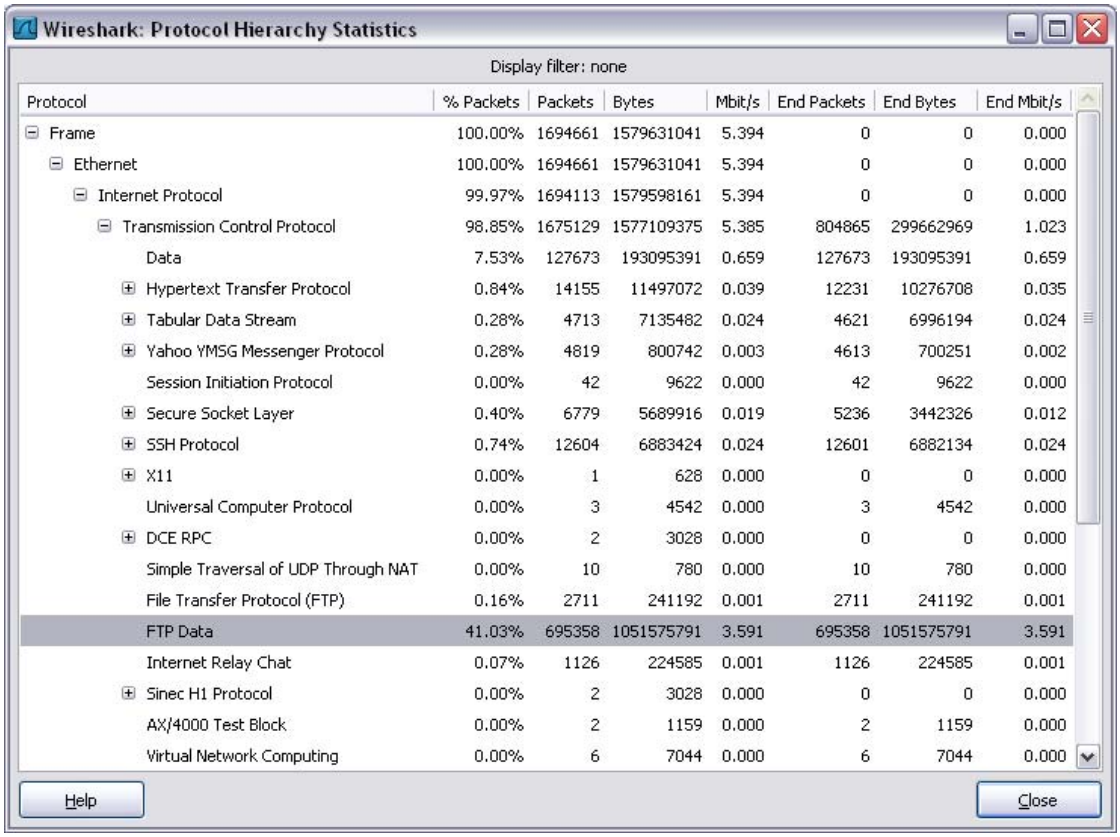

Figure 5: Protocol of UGM gateway (2 June 2008)

The figure 5 shows that FTP protocol is the most significant in use, encouraging the three server destination mentioned, which is used to upload and download huge file to and from the UGM local server.

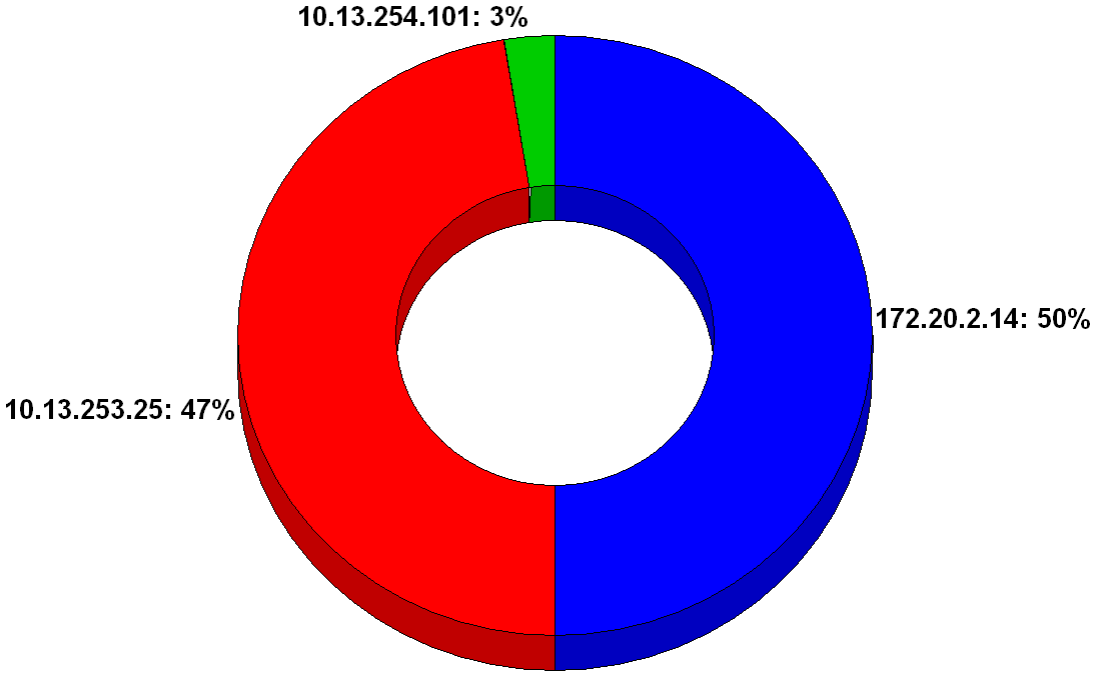

Figure 6: IP Destinations (Donut Mode)

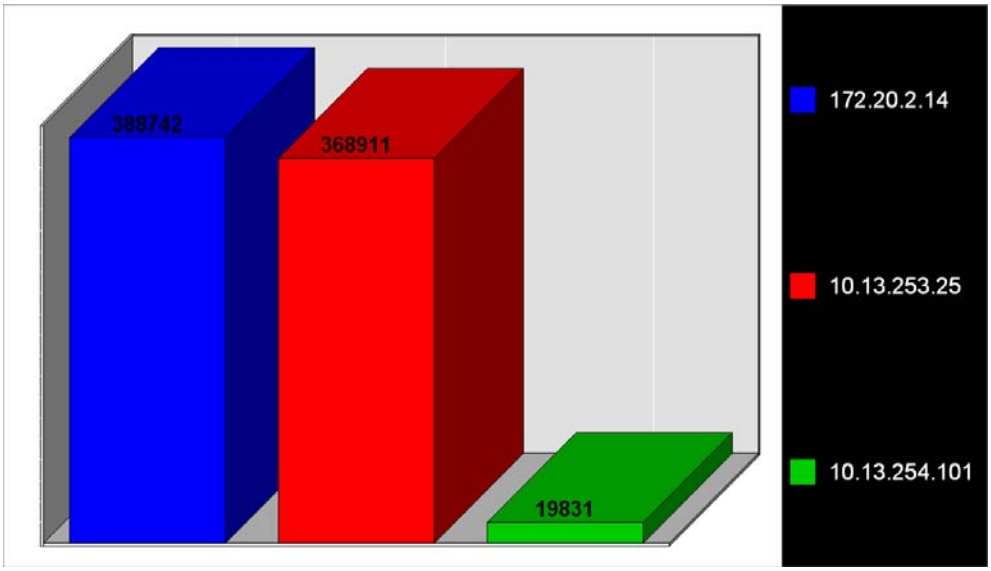

Figure 7: IP Destinations (Graph Mode)

Figure 6 and 7 show IP destination figure which is captured with another protocol analyzer (iris) in 3 June 2008. The result is not significantly different even indicate fairly same pattern with the result in 2 June 2008. The results are listed as follows.

1. 10.13.253.25 = (47%), UGM Local Server
2. 172.20.2.14 = (50%) FTP TE Server

This monitoring result show the same problem about the three local servers, which can cause ineffective performance of TE UGM networks services.

Date	Time	(1280-2559) byte	(80-159) byte	(40-79) byte	Others
2 June 2008	10.00	59,19 %	2,66 %	36,51 %	1,64 %
4 June 2008	09.00	61,07 %	2,61 %	35,56 %	0,76 %
6 June 2008	09.00	65,60 %	1,44 %	32,26 %	0,7 %
9 June 2008	11.00	67,50 %	0,94 %	30,40 %	1,16 %
12 June 2008	13.00	60,67 %	2,52 %	35,83 %	0,98 %

Figure 8: Size distribution in gateway UGM

Size distribution is the mean size of packets which is entered UGM gateway. The size of packets can indicate the types of files and the table result indicates that the most significant packet is (1280-2559) byte; it is typical for audio and video file.

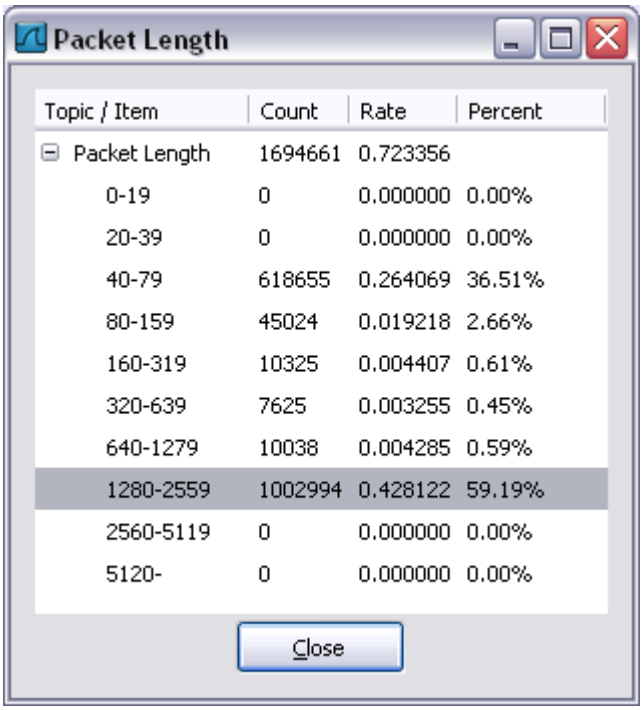

Figure 9: Sample of Gateway packet length (2 June 2008)

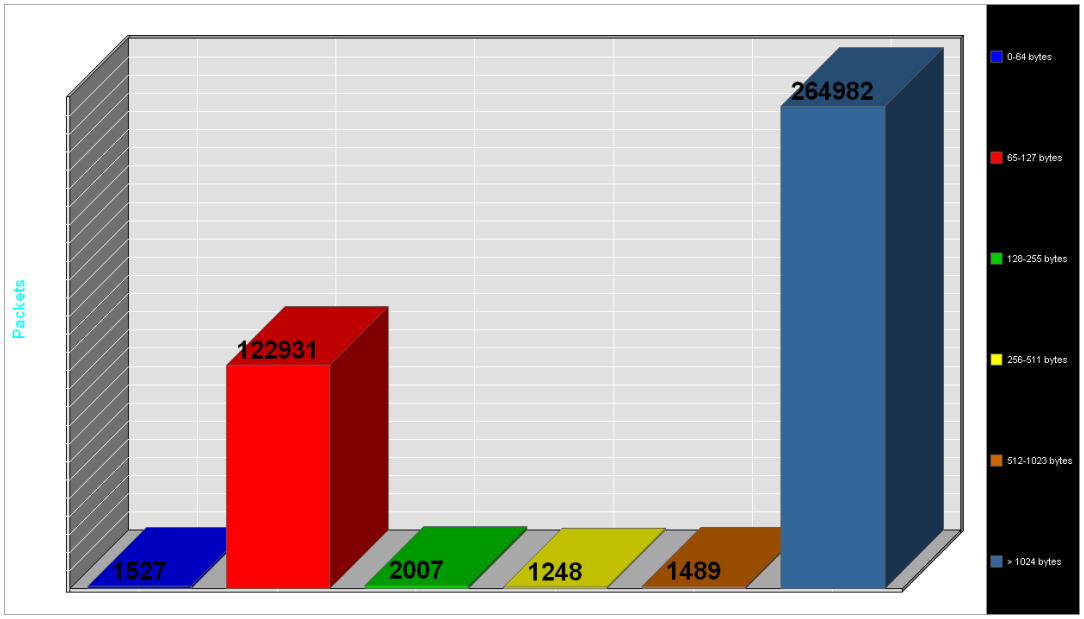

Figure 10: Sample of Size Distribution (Graph Mode) 3 June 2008

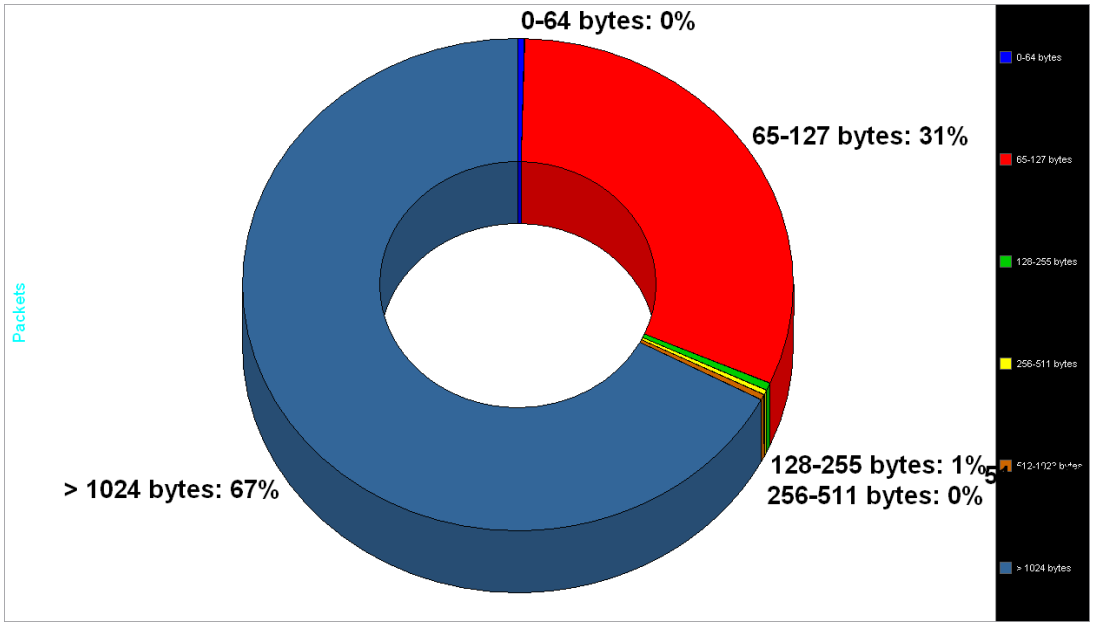

Figure 11: Sample of Size Distribution (Donut Mode) 3 June 2008

Figure 10 and 11 are sample of size distribution which is captured in 3 June 2008 at 10.00 am. The packet, which is >1024 bytes, is the most significant with 67%, another significant is 65-127 bytes 31%. It is also typical for audio and video file.

4.1.2. Problem Solution of Gateway T.E. UGM

From the results of monitoring, known that the network access mostly to and from 3 main servers which are contained huge entertainment files. The students usually download and upload huge entertainment files especially within working hour. Definitely, this activity is not appropriate with educational activity and can decrease the quality of communal educational activity; moreover it can cause the crowd traffic, disturb other network services which are appropriate with educational activity, even can cause network outages and disturb the performance of network services which is relevant with educational activity.

Therefore the system needs application to reduce the upload/download activity which is not appropriate with communal education especially within working hour 08.00 am – 04.00 pm, and set to be normal again when the working hour has been passed, because somehow it is also important to provide the necessary of entertainments for the students.

One of possible applications to limit unimportant access is ACLs (access control lists), an application in router, which is permit or deny the traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet.

A sample of simple commands is listed as follow.

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

To deny inappropriate traffics, permit can be changed with deny.

This condition can be applied for some part of time period, such as in working hour only and other than working hour the application will be changed to normal mode, it can be applied with Time-based ACLs, with a sample of simple commands is listed as follow.

```
R1(config)#time-range EVERYOTHERDAY
R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to
17:00

R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255
any eq telnet time-range EVERYOTHERDAY

R1(config)#interface s0/0/0
R1(config-if)#ip access-group 101 out
```

Thus, the application can increase the performance with restrict the traffic which is not appropriate with communal education, therefore any traffic which is appropriate with communal education can be increased its performance.

Another alternative application is management bandwidth method, which divide the priority of users and application as well as the necessary of the institution as educational institution. The example shows in figure 12.

Fasilitas	*Maks user*	*Alokasi*	*Status*	*Bandwidth (kbps)*	*Total (kbps)*
HTTP	30	25%		512	128
SMTP	50	75%		64	48
POP3	50	15%		512	76,8
FTP	20	10%		512	51,2
Other	10	15%		512	76,8
Squid	50	64%		10000	6400

Figure 12: A sample of bandwidth management.

Communal education activity mostly use SMTP protocol, therefore this protocol is given first priority, different with FTP which is given the lowest priority, because this protocol is mostly not appropriate with education activity.

4.2. Server Respond

Respond server is a parameter to measure how successful a server to request service. The bigger value is the better performance of the server to request the services.

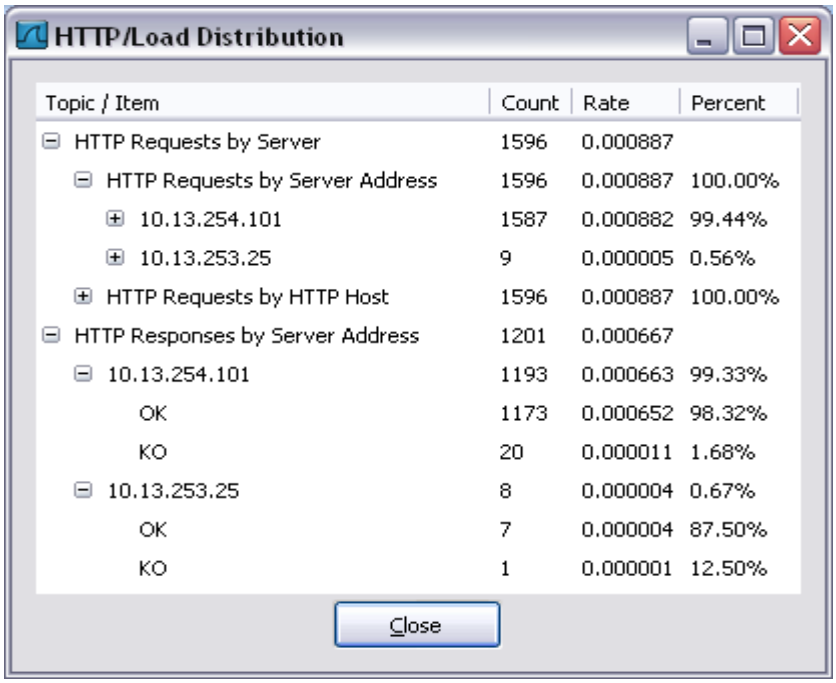

Figure 13: A Sample of Respond Server (1 July 2008, 11.00)

Server	Date	Jam	Success	Fail
10.13.254.101	1 July 2008	11.00	98,32%	1,68%
10.13.253.25	1 July 2008	11.00	87,50%	12,50%
10.13.254.101	3 July 2008	10.00	98,56%	1,44%
10.13.254.101	7 July 2008	13.00	98,34%	1,66%
10.13.254.101	8 July 2008	09.00	97,96%	2,04%
10.41.13.1	8 July 2008	09.00	100%	-
10.13.254.101	10 July 2008	10.00	98,11%	1,89%
10.41.13.1	10 July 2008	10.00	100%	-
10.13.254.101	11 July 2008	09.00	98,61%	1,39%
10.13.254.101	15 July 2008	09.30	97,92%	2,08%

Figure 14: Summary of Respond Server

The figure 14 shows that the respond server in UGM environment is good enough with the extreme lowest value is 87, 50%. Therefore, it does not need any reconfiguration in respond server field in order to optimize the networks services.

4.3 Proxy T.E.

4.3.1. Monitoring Results of Proxy TE

One of networks policy in Electrical Engineering Gadjah Mada University is compulsory to use proxy for any users, either proxy T.E. or proxy MTI. Therefore monitoring of proxy is the most significant way to obtain the pattern of traffic and the pattern of user's behavior, especially proxy T.E. which has the largest users in TE UGM.

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	[redacted]	795	3.03G	23.56%	0.05%	70.83%	04:02:06	14.52M	0.54%
2	[redacted]	1.48K	2.31G	18.01%	0.08%	92.64%	24:09:21	86.96M	3.25%
3	[redacted]	20.17K	1.54G	11.98%	0.83%	99.17%	127:18:53	458.33M	17.12%
4	[redacted]	433	1.50G	11.72%	0.02%	99.98%	01:25:12	5.11M	0.19%
5	[redacted]	2.15K	919.56M	7.14%	0.33%	99.67%	02:30:06	9.00M	0.34%
6	[redacted]	792	740.83M	5.76%	0.28%	99.72%	02:07:06	7.62M	0.28%
7	[redacted]	41	735.29M	5.71%	0.00%	100.00%	00:31:19	1.87M	0.07%
8	[redacted]	18	467.57M	3.63%	0.00%	100.00%	02:05:23	7.52M	0.28%
9	[redacted]	45	210.17M	1.63%	0.18%	99.82%	00:03:45	225.71K	0.01%
10	[redacted]	759	131.77M	1.02%	0.00%	100.00%	09:27:34	34.05M	1.27%
11	tamu	11.00K	107.79M	0.84%	12.85%	87.15%	30:04:45	108.28M	4.04%
12	[redacted]	2.43K	64.30M	0.50%	16.01%	83.99%	10:03:07	36.18M	1.35%
13	[redacted]	6.60K	57.92M	0.45%	4.98%	95.02%	160:08:27	576.50M	21.53%
14	[redacted]	666	55.58M	0.43%	0.62%	99.38%	04:52:00	17.52M	0.65%
15	[redacted]	1.32K	51.15M	0.40%	2.11%	97.89%	03:47:48	13.66M	0.51%
16	[redacted]	1.72K	37.79M	0.29%	15.11%	84.89%	12:10:30	43.83M	1.64%
17	[redacted]	2.51K	37.34M	0.29%	2.40%	97.60%	07:57:10	28.63M	1.07%
18	[redacted]	4.00K	32.43M	0.25%	20.97%	79.03%	04:09:10	14.95M	0.56%

Figure 15: User Rangking of proxy T.E.

From monitoring with proxy squid, figure 15 shows that there is no limit for using of internet connection, which is indicated that many users use connection with extreme very long time even exceed 160 hours continuously. Definitely, it is unusual habit and need investigation and concern about security problem. This unusual occurrence can be a potential threat source, which can cause many security problems. Therefore a limitation of connection is needed to prevent the system from security threat.

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
10.13.253.25	18	3.02G	99.72%	0.00%	100.00%	01:38:27	5.90M	40.67%
download.tune-up.com	6	4.64M	0.15%	0.00%	100.00%	01:26:30	5.19M	35.73%
images.friendster.com	193	785.57K	0.03%	32.78%	67.22%	00:09:14	554.70K	3.82%
divine-music.net	3	551.04K	0.02%	99.88%	0.12%	00:00:05	5.06K	0.03%
www.friendster.com	43	444.74K	0.01%	0.00%	100.00%	00:08:15	495.78K	3.41%
photos.friendster.com	66	353.52K	0.01%	18.54%	81.46%	00:07:56	476.17K	3.28%
www.liputan6.com	63	124.10K	0.00%	86.22%	13.78%	00:00:17	17.08K	0.12%
profiles.friendster.com	11	109.20K	0.00%	0.00%	100.00%	00:02:13	133.98K	0.92%
partner.googleadservices.com	48	106.96K	0.00%	0.00%	100.00%	00:01:15	75.89K	0.52%
pagead2.googlesyndication.com	36	96.29K	0.00%	0.00%	100.00%	00:01:07	67.11K	0.46%
static.liputan6.com	10	74.17K	0.00%	100.00%	0.00%	00:00:00	28	0.00%
ads.suryacitra.com	17	56.52K	0.00%	0.00%	100.00%	00:00:37	37.90K	0.26%
10.41.13.1	57	53.21K	0.00%	28.10%	71.90%	00:00:00	247	0.00%
sb.google.com	3	49.27K	0.00%	0.00%	100.00%	00:01:07	67.93K	0.47%
10.13.8.88	7	47.34K	0.00%	93.65%	6.35%	00:05:59	359.67K	2.48%
www.google-analytics.com	20	42.61K	0.00%	0.00%	100.00%	00:00:35	35.86K	0.25%
blumewahabi.files.wordpress.com	1	42.09K	0.00%	0.00%	100.00%	00:00:30	30.48K	0.21%
img6.cdn.adjuggler.com	2	42.01K	0.00%	100.00%	0.00%	00:00:00	3	0.00%
photos-p.friendster.com	4	38.25K	0.00%	0.00%	100.00%	00:01:49	109.67K	0.75%
www.boomspeed.com	1	26.90K	0.00%	0.00%	100.00%	00:00:14	14.96K	0.10%

Figure 16: a sample of common users' activity.

Figure 16 shows that there is no limit to use bandwidth especially within working hour; a user can download any contents without limit of file size. It can cause the very crowd traffic and disturb the connections especially within working hour. Moreover the download activity is not appropriate with educational framework and definitely will disturb the people who are in progress of educational activity.

NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	shttp.msg.yahoo.com	11.34K	6.86M	43.11M
2	85.131.179.6	10.02K	2.73M	228
3	ref.te.ugm.ac.id	7.23K	35.53M	532.83K
4	mail.google.com	4.41K	21.67M	103.75M
5	www.duniasex.com	3.94K	11.05M	6.94M
6	images.friendster.com	3.76K	9.44M	9.02M
7	kcpr.vp.video.l.google.com	3.34K	23.62M	298.05M
8	ad.detik.com	2.97K	24.73M	3.49M
9	te.ugm.ac.id	2.79K	9.67M	108.20K
10	pagead2.googlesyndication.com	2.79K	7.76M	9.68M
11	mozilla-mirror.internap.com	2.77K	12.41M	30.07M
12	www.google-analytics.com	2.34K	2.01M	6.45M
13	www.bb17.info	2.20K	8.47M	415.83K
14	tbn0.google.com	2.14K	9.79M	17.08M
15	74.125.96.35	1.96K	6.14M	170.51M

Figure 17: Top sites T.E.

The table from figure 17 shows that porn sites are still significant appeared, definitely it is illegal activity even implied in law transgression activity. Moreover, the sites which are not appropriate with educational activity are still also significant. It is evidenced that there is no limit for non educational sites especially within working hour and of course it will disturb the traffic.

4.3.2. Monitoring Results of Proxy MTI

Proxy MTI is a proxy for MTI students including MTI regular and CIO class.

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	[redacted]	253.22K	15.16G	52.36%	3.44%	14.16%	292:17:39	1.05G	42.95%
2	[redacted]	698.00K	7.07G	24.42%	10.91%	30.36%	130:30:12	469.81M	19.18%
3	[redacted]	24.44K	2.56G	8.84%	1.29%	83.83%	46:54:31	168.87M	6.89%
4	[redacted]	1.18M	642.39M	2.22%	80.97%	19.03%	10:15:58	36.95M	1.51%
5	[redacted]	7.81K	484.77M	1.67%	13.59%	86.41%	19:17:25	69.44M	2.83%
6	[redacted]	57.74K	357.02M	1.23%	25.23%	74.77%	16:28:51	59.33M	2.42%
7	172.20.2.14	6.10K	350.16M	1.21%	98.69%	1.31%	03:32:02	12.72M	0.52%
8	172.20.2.1	5.16K	315.50M	1.09%	99.28%	0.72%	02:20:23	8.42M	0.34%
9	[redacted]	3.13K	213.08M	0.74%	3.77%	96.23%	06:16:57	22.61M	0.92%
10	[redacted]	2.74K	210.00M	0.72%	57.83%	42.17%	03:30:13	12.61M	0.51%
11	[redacted]	1.92K	180.98M	0.62%	71.73%	28.27%	01:30:02	5.40M	0.22%
12	[redacted]	1.14K	113.83M	0.39%	30.65%	69.35%	04:37:55	16.67M	0.68%
13	[redacted]	3.28K	98.06M	0.34%	8.65%	91.35%	07:35:28	27.32M	1.12%
14	[redacted]	3.70K	93.72M	0.32%	11.57%	88.43%	10:29:21	37.76M	1.54%
15	172.20.2.2	334	79.95M	0.28%	99.97%	0.03%	00:00:14	14.47K	0.00%

Figure 18: MTI Top users.

Figure 18 shows similar problem with Proxy TE. There is also no limit time to use network services, which is indicated that some users be able to use connection in extreme very long time even exceed 292 hours nonstop and identified that the problem occurs because management password and security concern, which is indicated that it is counterfeit users because it is impossible if the real users be able to do connection more than 292 hours nonstop in campus area.

NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	www57.megaupload.com	1.18M	556.86M	13.45M
2	fs.vnmanga.com	617.50K	652.19M	19.60M
3	backtrack.mirrors.skynet.be	47.52K	96.25M	16.03M
4	static.ak.fbcdn.net	19.60K	82.04M	2.83M
5	shttp.msg.yahoo.com	14.80K	9.47M	34.68M
6	images.friendster.com	13.62K	28.33M	3.32M
7	www.kapanlagi.com	12.32K	12.74M	1.70M
8	pagead2.googlesyndication.com	10.20K	22.61M	7.46M
9	my.padmanaba.or.id	9.63K	21.70M	3.20M
10	www.google-analytics.com	9.17K	7.12M	4.88M
11	10.13.253.25	9.13K	14.19G	38.15M
12	profile.ak.facebook.com	5.73K	19.13M	2.98M
13	mail.google.com	5.71K	23.49M	116.18M
14	openx.detik.com	5.64K	13.87M	45.64M
15	kona.kontera.com	5.20K	6.08M	467.48K

Figure 19: MTI top sites.

Figure 19 also shows similar problem with Proxy TE, indicated that the sites which is not appropriate with educational activity is still significant. Therefore, the better management traffic is needed to solve this problem and to optimize the network services.

4.3.3. Problem Solution of Proxy TE and Proxy MTI

Basically, Proxy has two main functions. First, as cache function for connection efficiency because the proxy can be a temporary storage for any network services activity, which make the services not always to request services to internet public if the proxy has saved the content of services in its cache. The second, as a filter of any forbidden content which enter the traffic of networks system, therefore the proxy can enforce the network policy and can act as security device.

Based on proxy TE and proxy MTI monitoring, indicated that the proxies are not already optimum as its functions. Some problem are indicated such as, there is no limit for time connection, some of users are be able to connect the internet services with extreme very long time even exceed 292 hours nonstop. Of course, it ought to be limited due to efficiency and communal security concern. Furthermore, there is also no limit for size capacity of upload and download contents, many users are be able to download or upload with very huge file, actually it is legal and it does not matter if it is done in outside of working hour, it become a problem if it is done within working hour, because can cause the crowd traffic and disturb the performance of communal educational activity, therefore it need to be limited for efficiency reason. Moreover, porn sites are still a serious problem and the proxy setting need to update to prevent this activity.

Porn sites accesses are illegitimacy activity especially in educational institution, therefore the proxy ought to be reconfigure its current setting, such as adding the content from forbidden-domain.txt, forbidden-words.txt, and forbidden-ip.txt in directory /etc/squid.

```
# cd /etc/squid
# touch forbidden-domain.txt
# touch forbidden-words.txt
# touch forbidden-ip.txt
```

```
# vi forbidden-domain.txt
17tahun.com
www.playboy.com
www.nude.com
www.sex.com
www.porn.com
www.hardcore.com
And so on until enough.
```

```
# vi forbidden-words.txt
sex
xxx
hot
17tahun
Porn
And so on until enough.
```

```
# vi forbidden-ip.txt
70.84.171.179
216.163.137.3
64.74.96.243
209.81.7.23
213.193.215.179
216.130.180.165
And so on until enough.
```

If felt that it is not sufficient, using redirector SquidGuard application is another alternative, with this application, manual adding for forbidden-domain.txt, forbidden-words.txt, and forbidden-ip.txt in directory proxy are not needed anymore, because SquidGuard database has already provided very huge number any forbidden contents obtained with scripts robots, which is made from pearl language.

There is no limit for download size, time connection, inappropriate content with communal education are other serious problems in the networks system, especially in range of working hour because it can disturb others important communal education activity. Therefore some restrictions within working hour (08.00 am – 04.00 pm) are

needed to strengthen the important networks services and set to be normal again within outside of working hour.

A sample command as follows.

acl notfree download time 08:00am-04.00pm

acl magic_words2 url_regex
-i ftp .exe .mp3 .vqf .tar.gz
.gz .tar.bz2 .bz2 .rpm .zip
.rar .avi .mpeg .mpe .mpg .qt
.ram .rm .raw .wav .iso

Cancel download if file is
bigger than 10MB = 10000 X 1024
byte = 10240000 byte
reply_body_max_size 10240000 allow magic_words2 notfree download

This rule only permit maximum download quota for 10MB and be valid within working hour (08.00 am – 04.00 pm), the determination of maximum quota download can be change to more or less than 10MB depends on the policy and the agreement between management and users.

Another problem is many users can do connection in very extreme long time even exceed 292 hours nonstop, it can be solved with proxy application, the proxy can be also used to limit the length of connection, for example only 10 hours in a day except for any communal education or researches activity. Furthermore to strengthen the system and for better management, the networks need a new device, which is Radius Sever with AAA (authentication, authorization, and accounting). Therefore the password problems mentioned in monitoring results can be decreased.

4.4. Wireless Networks

Wi-Fi networks are Vlans which have the biggest number of users in Faculty of Electrical Engineering Gadjah Mada University. Therefore, Monitoring in these Vlan is also important to obtain better data to identify the problems.

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	305934	280527176	4.288	0	0	0.000
Ethernet	100.00%	305934	280527176	4.288	0	0	0.000
Internet Protocol	100.00%	305926	280526840	4.288	1	110	0.000
Transmission Control Protocol	99.96%	305818	280509769	4.288	125278	7265300	0.111
Hypertext Transfer Protocol	59.00%	180501	273238810	4.177	180484	273224757	4.177
Yahoo YMSG Messenger Protocol	0.00%	13	1733	0.000	12	1385	0.000
Secure Socket Layer	0.00%	10	1400	0.000	10	1400	0.000
NetBIOS Session Service	0.01%	16	2526	0.000	2	184	0.000
User Datagram Protocol	0.03%	107	16961	0.000	0	0	0.000
Address Resolution Protocol	0.00%	8	336	0.000	8	336	0.000

Figure 20: Protocol Hierarchy statistics of wireless Networks.

Figure 20 shows that protocol HTTP is the biggest using in the networks (59%), which is appropriate with the problems which show in the proxy data. It encourages the conclusion about the users' pattern and behavior which is frequently to do uncommon activity with educational fields.

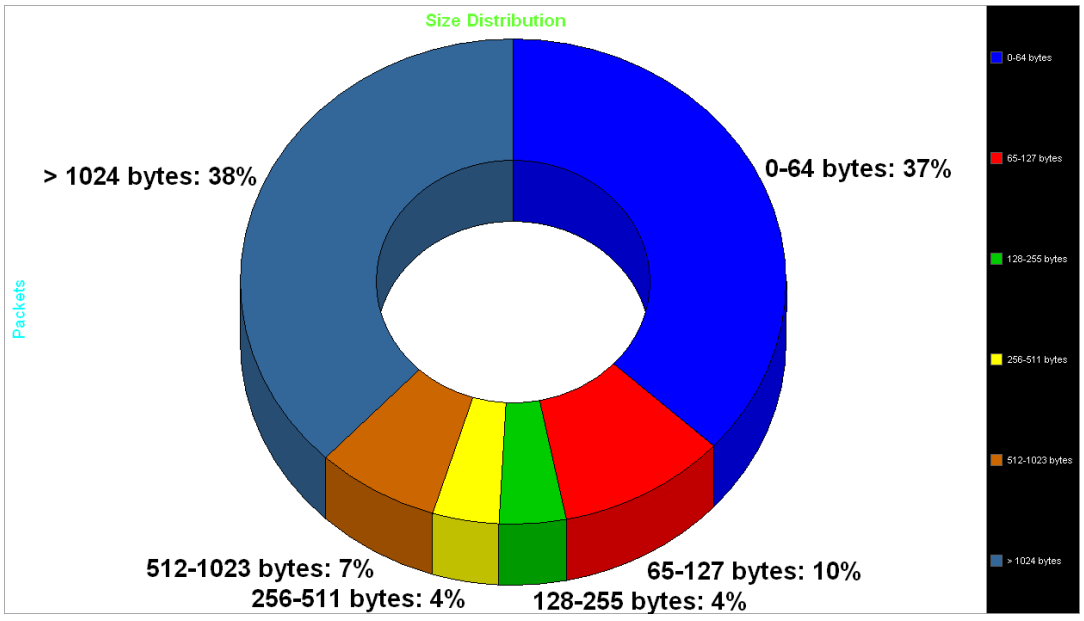

Figure 21: Size distribution of wireless networks.

Figure 21 shows that the biggest number of packet size is >1024 bytes with 38%, it encourages the data from the gateway which is indicated that the users' activity mostly in communal entertainments, such as audio and video file. Definitely, it can disturb the traffic which is relevant with educational activity. All of the problems in wireless networks have been solved in proxy chapter. Therefore for a while, this chapter does not need problem solution.

5. Conclusions and Future works

As the results from monitoring and problem solutions, the conclusions and future works are listed as follows.

1. Based on respond server parameter, performance of networks services in TE UGM is good enough; it is indicated from monitoring results that the successful respond server is within 87%-100%.

2. The performance of proxies, both TE proxy and MTI proxy are not satisfy enough which is indicated that the porn sites is still significant from monitoring results, furthermore there is no limit for time connection even many users can connect until more than 292 hours continuously, moreover there is no limit for the large of file size, especially within working hour as the most crowd traffic. Therefore, the proxies need to be reconfigured to optimize the use of bandwidth especially within working hour.

3. Network management in TE UGM networks services also need to reformulate, including ACLs to list the priority of users for communal educational activity, bandwidth allocation for optimization, and for security concern.

4. To strengthen the security system and to optimize the networks services, network policy must be reformulated to meet the optimization as educational institution. Therefore, Network policy can be the future work, which is concern about how to formulate network policy in educational institution. Another future work is how to manage security concern in educational institution.

Bibliography

[1] A.Ciuffoletti and M. Polychronakis. Architecture of a network monitoring element. Technical Report TR-0033, CoreGRID Project. 2006.

[2] A.Eryilmaz and R. Srikant, “Fair resource allocation in wireless networks using queue-length-based scheduling and congestion control,” in Proceedings of IEEE INFOCOM, 2005.

[3] A.Eryilmaz and R. Srikant, “Joint Congestion Control, Routing and MAC for Stability and Fairness in Wireless Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 8, pp. 1514–1524, August 2006.

[4] A.Moore and K. Papagiannaki. Toward the accurate identification of network applications. In *Passive and Active Measurement Workshop*, Boston, MA, USA, 2005.

[5] A.Ramachandran, S. Seetharaman, and N. Feamster. Fast Monitoring of Traffic Sub- populations. In Proc. IMC, 2008.

[6] Alistair Phipps. Network performance monitoring architecture. Technical Report EGEE-JRA4-TEC-606702- NPM NMWG Model Design, JRA4 Design Team, September 2005.

[7] Antonis Papadogiannakis, Alexandros Kapravelos,Michalis Polychronakis, Evangelos P.Markatos, and Augusto Ciuffoletti. Passive end-to-end packet loss estimation for grid traffic monitoring. In *Proceedings of the CoreGRID Integration Workshop*, 2006.

[8] Augusto Ciuffoletti, Antonis Papadogiannakis, and Michalis Polychronakis. Network monitoring session description. In *CoreGRID Workshop at the International Supercomputing Conference*, page 15, Dresden, June 2007.

[9] D. Antoniades, M. Polychronakis, S. Antonatos, E. P. Markatos, S. Ubik, and A. Oslebo, "Appmon: An application for accurate per application traffic characterization," in *Proceedings of IST Broadband Europe Conference*, 2006.

[10] D. X. Wei, C. Jin, S. H. Low, and S. Hegde, "FAST TCP: motivation, architecture, algorithms, performance," IEEE/ACM Transactions on Networking, Dec. 2006.

[11] F. Hernandez-Campos and M. Papadopouli. A comparative measurement study of the workload of wireless access points in campus networks. In *16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications*, Berlin, Germany, September 2005.

[12] F. Hernandez-Campos, M. Karaliopoulos, M. Papadopouli, and H. Shen. Spatio-temporal modeling of traffic workload in a campus WLAN. In *Second Annual International Wireless Internet Conference*, Boston, USA, August 2006.

[13] H. Ballani and P. Francis. CONMan: A Step Towards Network Manageability. In Proc. ACM SIGCOMM, 2007.

[14] H. Veiga, T. Pinho, J. L. Oliveira, R. Valadas, P. Salvador, and A. Nogueira, "Active traffic monitoring for heterogeneous environments," *Proceedings of 4th International Conference on Networking (ICN05), Reunion Island*, vol. 2005, April.

[15] J. Bicket, D. Aguayo, S. Biswas, and R. Morris. Architecture and evaluation of an unplanned 802.11b mesh network. In *ACM International Conference on Mobile Computing and Networking (MobiCom)*, Cologne, Germany, August 2005.

[16] K. Xu, Z. Zhang, and S. Bhattacharyya. Profiling Internet Backbone Traffic: Behavior Models and Applications. In ACM SIGCOMM, 2005.

[17] L. Bui, R. Srikant, and A. L. Stolyar, "Optimal resource allocation for multicast flows in multihop wireless networks," in Proceedings of the IEEE Conference on Decision and Control, December 2007.

[18] M. Crovella and B. Krishnamurthy. Internet Measurement: Infrastructure, Traffic and Applications. John Wiley and Sons, Inc, 2006.

[19] M. Karaliopoulos, M. Papadopouli, E. Raftopoulos, and H. Shen. On scalable measurement-driven modeling of traffic demand in large wlans. Technical Report 383, ICS-FORTH, Heraklion, Crete, Greece, August 2006.

[20] M. Papadopouli, H. Shen, and M. Spanakis. Characterizing the duration and association patterns of wireless access in a campus. In *11th European Wireless Conference*, Nicosia, Cyprus, April 2005.

[21] M. R. Sharma and J. W. Byers. Scalable Coordination Techniques for Distributed Network Monitoring. In Proc. PAM, 2005.

[22] Panos Trimintzios, Michalis Polychronakis, Antonis Papadogiannakis, Michalis Foukarakis, Evangelos P. Markatos, and Arne Øslebø. DiMAPI: An application programming interface for distributed network monitoring. In *Proceedings of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2006.

[23] S.Andreozzi, D.Antoniades, A.Ciu®oletti, A.Ghiselli, E.P.Markatos, M.Polychronakis, and P.Trimintzios. Issues about the integration of passive and active monitoring for grid networks. In CoreGRID Integration Workshop 2005.

[24] V. Sekar, M. K. Reiter, W. Willinger, H. Zhang, R. Kompella, and D. G. Andersen. cSamp: A System for Network-Wide Flow Monitoring. In Proc. NSDI, 2008.

[25] X. Lin, N. Shroff, and R. Srikant, "A tutorial on cross-layer optimization in wireless networks," IEEE Journal on Selected Areas in Communications, pp. 1452–1463, August 2006.