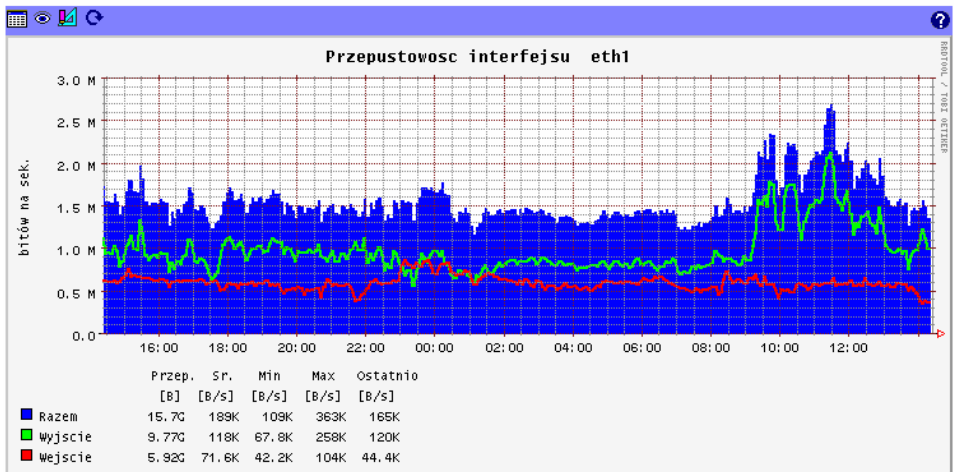
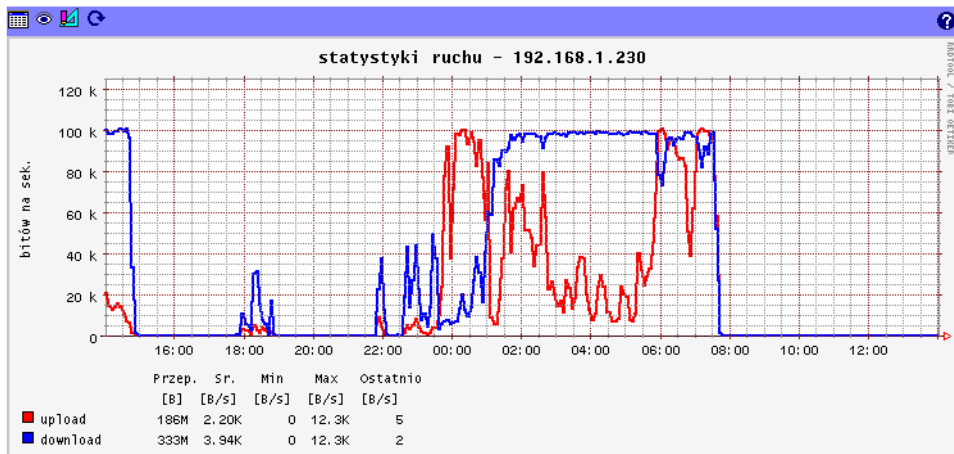


Serwer ISP – Monitorowanie ruchu

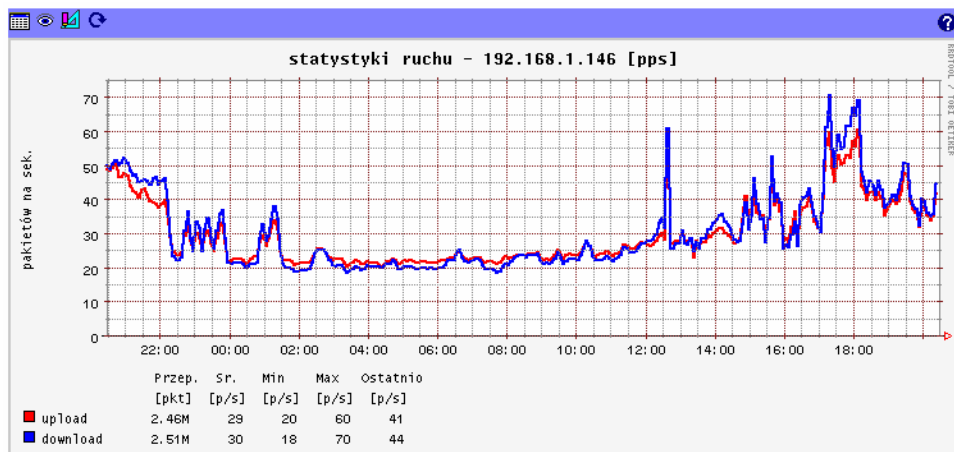
1. Statystyki graficzne



Rys.1. - Statystyki interfejsów sieciowych



Rys.2 - Statystyki użytkowników – transfer generowany przez użytkownika w bit/s



Rys.3 - Statystyki użytkowników - transfer generowany przez użytkownika w pkt/s

2. Statystyki tabelkowe

Year: 2005 2006
 Month: 01
 Day: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Statistics: [daily | day-in-month | monthly | month-in-year | yearly | year-in-global | global]

Statistics for day 23-01-2006

| Lp. | Host | In | Out | Total |
|-----|---------------|-----------|------------|-----------|
| 1. | 192.168.1.146 | 103.73 MB | 133.41 MB | 237.15 MB |
| 2. | 192.168.1.238 | 60.93 MB | 63.92 MB | 124.86 MB |
| 3. | 192.168.1.177 | 36.82 MB | 1.87 MB | 38.68 MB |
| 4. | 192.168.1.175 | 34.68 MB | 44.3 MB | 78.99 MB |
| 5. | 192.168.1.200 | 28.84 MB | 9.44 MB | 38.28 MB |
| 6. | 192.168.1.121 | 20.71 MB | 10.89 MB | 31.6 MB |
| 7. | 192.168.1.188 | 7.82 MB | 34.6 MB | 42.42 MB |
| 8. | 192.168.1.230 | 6.25 MB | 9.25 MB | 15.5 MB |
| 9. | 192.168.1.190 | 6.21 MB | 198.91 kB | 6.4 MB |
| 10. | 192.168.1.183 | 3.94 MB | 175.28 kB | 4.12 MB |
| 11. | 192.168.1.203 | 3.37 MB | 9.11 MB | 12.48 MB |
| 12. | 192.168.1.156 | 3.32 MB | 10.56 MB | 13.88 MB |
| 13. | 192.168.1.197 | 2.96 MB | 264.37 kB | 3.22 MB |
| 14. | 192.168.1.195 | 2.56 MB | 757.33 kB | 3.3 MB |
| 15. | 192.168.1.181 | 2.31 MB | 1008.19 kB | 3.29 MB |
| 16. | 192.168.1.233 | 2.26 MB | 518.27 kB | 2.77 MB |
| 17. | 192.168.1.179 | 413.32 kB | 131.76 kB | 545.08 kB |
| 18. | 192.168.1.189 | 389.69 kB | 421.89 kB | 811.58 kB |
| 19. | 192.168.1.222 | 243.26 kB | 48.09 kB | 291.35 kB |
| 20. | 192.168.1.231 | 240 kB | 26.36 kB | 266.36 kB |
| 21. | 192.168.1.219 | 239.07 kB | 144.06 kB | 383.12 kB |
| 22. | 192.168.1.255 | 176.53 kB | 0 b | 176.53 kB |
| 23. | 192.168.1.120 | 159.07 kB | 0 b | 159.07 kB |
| 24. | 192.168.1.232 | 131.39 kB | 131.35 kB | 262.74 kB |
| 25. | 192.168.1.154 | 61.05 kB | 56.79 kB | 117.83 kB |

Rys.4. Tabelkowe statystyki dziennych/miesięcznych transferów użytkowników

3. Statystyki zapytań WWW



Squid User Access Reports

| PLIK/PRZEDZ. | DATA UTWORZ. | UŻYT. | Bajt. | ŚREDNIA |
|-------------------------------------|------------------------------|-------|-------|---------|
| 2006Jan23-2006Jan23 | wto sty 24 06:27:28 CET 2006 | 61 | 3G | 34M |
| 2006Jan22-2006Jan22 | pon sty 23 06:27:11 CET 2006 | 54 | 2G | 37M |
| 2006Jan21-2006Jan21 | nie sty 22 06:27:20 CET 2006 | 52 | 3G | 45M |
| 2006Jan20-2006Jan20 | sob sty 21 06:27:08 CET 2006 | 55 | 3G | 42M |
| 2006Jan19-2006Jan19 | pią sty 20 06:27:13 CET 2006 | 65 | 3G | 32M |
| 2006Jan18-2006Jan18 | czw sty 19 06:27:08 CET 2006 | 57 | 3G | 44M |
| 2006Jan17-2006Jan17 | śro sty 18 06:27:03 CET 2006 | 65 | 3G | 33M |
| 2006Jan16-2006Jan16 | wto sty 17 06:26:59 CET 2006 | 62 | 2G | 29M |
| 2006Jan15-2006Jan15 | pon sty 16 06:27:03 CET 2006 | 58 | 2G | 28M |
| 2006Jan14-2006Jan14 | nie sty 15 06:27:04 CET 2006 | 59 | 2G | 26M |
| 2006Jan13-2006Jan13 | sob sty 14 06:27:01 CET 2006 | 62 | 3G | 36M |
| 2006Jan12-2006Jan12 | pią sty 13 06:26:56 CET 2006 | 60 | 3G | 40M |
| 2006Jan11-2006Jan11 | czw sty 12 06:26:55 CET 2006 | 60 | 4G | 59M |
| 2006Jan10-2006Jan10 | śro sty 11 06:26:40 CET 2006 | 49 | 395M | 9M |
| 2006Jan09-2006Jan09 | wto sty 10 06:26:50 CET 2006 | 64 | 4G | 51M |
| 2006Jan08-2006Jan08 | pon sty 9 06:26:55 CET 2006 | 54 | 3G | 49M |
| 2006Jan07-2006Jan07 | nie sty 8 06:26:52 CET 2006 | 61 | 4G | 53M |
| 2006Jan06-2006Jan06 | sob sty 7 06:26:45 CET 2006 | 7313 | 25M | 3K |
| 2006Jan05-2006Jan05 | pią sty 6 06:26:33 CET 2006 | 6785 | 185M | 24K |
| 2006Jan04-2006Jan04 | czw sty 5 06:26:34 CET 2006 | 73 | 3G | 33M |
| 2006Jan03-2006Jan03 | śro sty 4 06:26:29 CET 2006 | 77 | 3G | 37M |
| 2006Jan02-2006Jan02 | wto sty 3 06:26:22 CET 2006 | 8146 | 201M | 25K |
| 2006Jan01-2006Jan01 | pon sty 2 06:26:16 CET 2006 | 56 | 3G | 49M |
| 2005Dec31-2005Dec31 | nie sty 1 06:26:14 CET 2006 | 52 | 3G | 46M |
| 2005Dec30-2005Dec30 | sob gru 31 06:26:17 CET 2005 | 64 | 4G | 47M |

Rys.5. - Archiwum statystyk



Squid User Access Reports
 Przedział czasowy: 2006Jan22-2006Jan22
 Sortowanie: BYTES, reverse
 Topuser Raport

Główne Serwisy Raport
 Serwisy & Użytkownicy Raport
 Graphic Raport
 Zabroniony Raport

| Nr | ID Użytk. | POŁĄCZENIA | Bajt. | %Bajt. | Wyj-CACHE-Wyj | CZAS UŻYTKOWANIA | MILISEK | %CZAS | |
|----|---------------|------------|-------|--------|---------------|------------------|----------|-------|--------|
| 1 | 192.168.1.177 | 47 | 430M | 21.90% | 0.00% | 100.00% | 07:09:45 | 26M | 4.16% |
| 2 | 192.168.1.171 | 18K | 375M | 19.10% | 4.34% | 95.66% | 31:31:21 | 114M | 18.29% |
| 3 | 192.168.1.179 | 3K | 258M | 13.15% | 1.43% | 98.57% | 04:28:59 | 17M | 2.60% |
| 4 | 192.168.1.215 | 5K | 150M | 7.64% | 2.26% | 97.74% | 04:40:25 | 17M | 2.71% |
| 5 | 192.168.1.200 | 18K | 107M | 5.41% | 2.78% | 97.22% | 74:44:19 | 270M | 43.37% |
| 6 | 192.168.1.146 | 13K | 62M | 3.15% | 23.78% | 76.22% | 02:00:48 | 8M | 1.17% |
| 7 | 192.168.1.106 | 2K | 53M | 2.68% | 2.32% | 97.68% | 01:56:51 | 8M | 1.13% |
| 8 | 192.168.1.203 | 5K | 42M | 2.12% | 7.32% | 92.68% | 02:27:24 | 9M | 1.43% |
| 9 | 192.168.1.219 | 8K | 25M | 1.26% | 24.58% | 75.42% | 00:59:04 | 4M | 0.57% |
| 10 | 192.168.1.222 | 5K | 24M | 1.20% | 8.75% | 91.25% | 01:45:57 | 7M | 1.02% |
| 11 | 192.168.1.120 | 2K | 23M | 1.17% | 6.06% | 93.94% | 00:19:08 | 2M | 0.19% |
| 12 | 192.168.1.159 | 5K | 23M | 1.17% | 7.56% | 92.44% | 01:27:18 | 6M | 0.84% |
| 13 | 192.168.1.121 | 4K | 23M | 1.15% | 5.64% | 94.36% | 01:51:03 | 7M | 1.07% |
| 14 | 192.168.1.233 | 7K | 22M | 1.09% | 36.35% | 63.65% | 00:13:35 | 2M | 0.31% |
| 15 | 192.168.1.234 | 3K | 22M | 1.08% | 11.49% | 88.51% | 01:09:14 | 5M | 0.67% |
| 16 | 192.168.1.148 | 3K | 21M | 1.03% | 3.33% | 96.67% | 03:53:10 | 14M | 2.26% |
| 17 | 192.168.1.225 | 4K | 20M | 0.97% | 31.41% | 68.59% | 00:42:47 | 3M | 0.41% |
| 18 | 192.168.1.180 | 3K | 18M | 0.90% | 9.96% | 90.04% | 00:31:24 | 2M | 0.30% |

Rys.6. - Statystyki zapytań użytkowników - zbiorowe



Squid User Access Reports
 Przedział czasowy: 2006Jan22-2006Jan22
 Użytkownik: 192.168.1.219
 Sortowanie: BYTES, reverse
 Użytk. Raport

| ODWIEDZONE SERWISY | POŁĄCZENIA | Bajt. | %Bajt. | Wyj-CACHE-Wyj | CZAS UŻYTKOWANIA | MILISEK | %CZAS | |
|------------------------|------------|-------|--------|---------------|------------------|----------|-------|--------|
| photos.allegro.pl | 1K | 7M | 26.71% | 3.99% | 96.01% | 00:07:27 | 448K | 12.63% |
| download.gadu-gadu.pl | 2 | 4M | 15.63% | 100.00% | 0.00% | 00:03:44 | 224K | 6.33% |
| www.caztuning.info | 201 | 2M | 5.24% | 34.62% | 65.38% | 00:07:02 | 423K | 11.93% |
| moto.allegro.pl | 642 | 2M | 4.86% | 9.76% | 90.24% | 00:02:15 | 135K | 3.81% |
| m.onet.pl | 178 | 922K | 3.73% | 0.90% | 99.10% | 00:01:12 | 73K | 2.05% |
| www.wiersze.bej.pl | 56 | 725K | 2.93% | 4.02% | 95.98% | 00:00:37 | 38K | 1.07% |
| www.lima.com.pl | 21 | 662K | 2.68% | 0.15% | 99.85% | 00:02:23 | 144K | 4.06% |
| teledyski.onet.pl | 142 | 544K | 2.20% | 1.93% | 98.07% | 00:00:51 | 51K | 1.45% |
| www.mago.republika.pl | 6 | 455K | 1.84% | 0.00% | 100.00% | 00:00:55 | 55K | 1.56% |
| adsearch.adkontekst.pl | 24 | 363K | 1.47% | 0.00% | 100.00% | 00:00:09 | 9K | 0.26% |
| www.gratka.pl | 141 | 319K | 1.29% | 17.24% | 82.76% | 00:00:24 | 24K | 0.68% |
| www.nc.pl | 18 | 293K | 1.19% | 0.00% | 100.00% | 00:00:25 | 26K | 0.72% |
| poczta06.o2.pl | 29 | 286K | 1.16% | 0.46% | 99.54% | 00:00:32 | 32K | 0.92% |
| appmsg.gadu-gadu.pl | 2K | 285K | 1.15% | 0.00% | 100.00% | 00:09:40 | 581K | 16.39% |
| adserver.gadu-gadu.pl | 200 | 272K | 1.10% | 0.00% | 100.00% | 00:00:26 | 26K | 0.74% |
| img.ale.gratka.pl | 126 | 256K | 1.03% | 10.17% | 89.83% | 00:00:15 | 16K | 0.44% |
| www.gadu-gadu.pl | 103 | 200K | 0.81% | 90.29% | 9.71% | 00:00:16 | 16K | 0.46% |
| www.o2.pl | 12 | 189K | 0.76% | 1.05% | 98.95% | 00:00:11 | 12K | 0.34% |
| sympatia.onet.pl | 31 | 188K | 0.76% | 0.00% | 100.00% | 00:00:11 | 11K | 0.32% |
| www.funt.inter-c.pl | 2 | 182K | 0.74% | 0.00% | 100.00% | 00:00:23 | 24K | 0.67% |
| www.rajdy.hoga.pl | 57 | 181K | 0.73% | 3.38% | 96.62% | 00:00:11 | 12K | 0.34% |
| img281.imageshack.us | 7 | 180K | 0.73% | 93.33% | 6.67% | 00:00:31 | 32K | 0.89% |
| adsearch.wp.pl | 34 | 171K | 0.69% | 0.00% | 100.00% | 00:00:02 | 3K | 0.08% |
| www.onet.pl | 62 | 171K | 0.69% | 59.33% | 40.67% | 00:00:07 | 7K | 0.20% |
| gaduk.ok.9x.pl | 37 | 167K | 0.68% | 0.00% | 100.00% | 00:00:16 | 16K | 0.47% |
| pogoda.onet.pl | 75 | 166K | 0.67% | 72.30% | 27.70% | 00:00:09 | 10K | 0.28% |

Rys.7. - Statystyki zapytań użytkownika – indywidualne

4. Statystyki bieżącego wykorzystania poszczególnych klas - w trybie konsoli

Statystyki klas usług:

mediaok-pkp:/# mon-htb down

01:28:00 up 7 days, 14:53, 2 users, load average: 0.11, 0.07, 0.01

| Dev | ClassID | ClassName | Tokens | Ctokens | Rate [bit/s/] | Ceil [bit/s] | Current | | | Cumulated Send [Byte] | Total Send [Byte] |
|------|---------|-----------|--------|---------|------------------|-----------------|-----------------|------------------|---------|-----------------------------|-------------------------|
| | | | | | | | Rate [bit/s] | Speed [bit/s] | [pkt/s] | | |
| imq0 | 3:1 | main | 8233 | 8376 | 3.70M | 3.70M | 598.46K | 638.53K | 138pps | 1.09MB | 696.42MB |
| imq0 | 3:10 | p2p | -12062 | 8873 | 100.00K | 1.00M | 554.86K | 577.48K | 118pps | 1023.27KB | 613.10MB |
| imq0 | 3:2 | internet | 11282 | 8445 | 2.70M | 2.70M | 596.78K | 638.53K | 138pps | 1.09MB | 696.19MB |
| imq0 | 3:3 | local | 39846 | 18258 | 1.00M | 1.00M | 16 | 0 | 0 | 0B | 227.78KB |
| imq0 | 3:4 | interakt | 198967 | 41571 | 200.00K | 300.00K | 2.53K | 1.01K | 5pps | 3.35KB | 3.30MB |
| imq0 | 3:5 | poczta | 200016 | 18415 | 200.00K | 1.00M | 0 | 10.59K | 6 | 6.50KB | 801.24KB |
| imq0 | 3:6 | www | 133344 | 15008 | 300.00K | 1.50M | 32.01K | 36.42K | 5pps | 56.00KB | 53.02MB |
| imq0 | 3:7 | ftp | 198443 | 18101 | 200.00K | 1.00M | 0 | 148 | 0 | 93B | 5.56KB |
| imq0 | 3:8 | gry | 199754 | 59048 | 200.00K | 200.00K | 0 | 0 | 0 | 0B | 586B |
| imq0 | 3:9 | inne | 390596 | 31393 | 100.00K | 400.00K | 9.36K | 12.88K | 13pps | 30.71KB | 25.85MB |

Statystyki klas użytkowników:

mediaok-pkp:/# mon2-htb down

19:55:44 up 3:20, 2 users, load average: 1.05, 0.79, 0.71

| Dev | ClassID | ClassName | Tokens | Ctokens | Rate [bit/s/] | Ceil [bit/s] | Current | | | Cumulated Send [Byte] | Total Send [Byte] |
|------|---------|-----------|----------|---------|------------------|-----------------|-----------------|------------------|---------|-----------------------------|-------------------------|
| | | | | | | | Rate [bit/s] | Speed [bit/s] | [pkt/s] | | |
| eth1 | 1:1 | main | 3703 | 5940 | 5.00M | 5.00M | 1.80M | 1.56M | 354pps | 28.56MB | 1.67GB |
| eth1 | 1:1022 | user | -1633806 | -35223 | 10.00K | 320.00K | 75.90K | 180.41K | 9pps | 410.11KB | 11.41MB |
| eth1 | 1:1023 | user | -1564338 | 34408 | 10.00K | 320.00K | 15.71K | 38.10K | 3pps | 146.22KB | 6.31MB |
| eth1 | 1:1024 | user | -784463 | -29648 | 10.00K | 320.00K | 248 | 17.17K | 0 | 12.79KB | 35.82KB |
| eth1 | 1:1027 | user | 3769303 | 33424 | 10.00K | 320.00K | 1.62K | 1.77K | 1pps | 8.16KB | 4.21MB |
| eth1 | 1:1028 | user | -2217344 | 71762 | 10.00K | 160.00K | 29.62K | 22.52K | 15pps | 116.24KB | 5.66MB |
| eth1 | 1:1041 | user | -3936357 | -54718 | 10.00K | 320.00K | 267.60K | 96.33K | 22pps | 1.17MB | 6.76MB |
| eth1 | 1:1045 | user | 3953131 | 38667 | 10.00K | 320.00K | 4.10K | 4.49K | 2pps | 18.79KB | 1.17MB |
| eth1 | 1:1052 | user | -51664 | -43408 | 10.00K | 320.00K | 313.48K | 315.84K | 28pps | 1.55MB | 90.23MB |
| eth1 | 1:1059 | user | 3970826 | 39977 | 10.00K | 320.00K | 20.69K | 2.83K | 4pps | 116.59KB | 1.76MB |
| eth1 | 1:1064 | user | -198825 | -818 | 10.00K | 320.00K | 51.49K | 40.97K | 12pps | 214.00KB | 59.82MB |
| eth1 | 1:1077 | user | -75675 | -24896 | 10.00K | 320.00K | 279.11K | 279.87K | 48pps | 1.34MB | 94.98MB |
| eth1 | 1:1081 | user | -4645278 | -18020 | 10.00K | 320.00K | 112.29K | 62.91K | 24pps | 447.06KB | 43.58MB |
| eth1 | 1:1086 | user | 3984588 | 39650 | 10.00K | 320.00K | 2.54K | 1.21K | 4pps | 12.66KB | 5.51MB |
| eth1 | 1:1087 | user | -180539 | 30802 | 10.00K | 320.00K | 16.32K | 29.52K | 3pps | 105.16KB | 3.36MB |
| eth1 | 1:1091 | user | -346842 | -60927 | 10.00K | 320.00K | 304.31K | 330.12K | 36pps | 1.56MB | 67.89MB |
| eth1 | 1:1098 | user | -620430 | -10484 | 10.00K | 320.00K | 136.12K | 61.16K | 13pps | 656.66KB | 33.21MB |
| eth1 | 1:1106 | user | 2607371 | 32606 | 10.00K | 320.00K | 23.08K | 8.17K | 4pps | 116.19KB | 2.08MB |
| eth1 | 1:1107 | user | 3565486 | 30639 | 10.00K | 320.00K | 1.81K | 2.85K | 0 | 8.29KB | 489.40KB |
| eth1 | 1:1114 | user | -236849 | -27359 | 10.00K | 320.00K | 115.70K | 69.11K | 13pps | 568.92KB | 28.79MB |
| eth1 | 1:1135 | user | 3995074 | 326042 | 10.00K | 32.00K | 4.46K | 85 | 0 | 769.38KB | 11.75MB |
| eth1 | 1:1146 | user | -670155 | 9995 | 10.00K | 320.00K | 57.70K | 45.39K | 22pps | 2.27MB | 101.55MB |
| eth1 | 1:1155 | user | -337121 | -123296 | 10.00K | 160.00K | 161.41K | 147.48K | 36pps | 6.60MB | 200.01MB |
| eth1 | 1:1159 | user | 3963617 | 106758 | 10.00K | 100.00K | 8.10K | 2.51K | 1pps | 415.91KB | 17.99MB |
| eth1 | 1:1161 | user | 3947888 | 68813 | 10.00K | 160.00K | 96 | 189 | 0 | 87.82KB | 4.25MB |
| eth1 | 1:1171 | user | 3995074 | 39977 | 10.00K | 320.00K | 120 | 773 | 0 | 5.97KB | 21.55MB |
| eth1 | 1:1175 | user | -2796278 | 27341 | 10.00K | 512.00K | 15.14K | 14.51K | 20pps | 388.80KB | 139.85MB |
| eth1 | 1:1177 | user | -1069864 | 34898 | 10.00K | 320.00K | 34.54K | 3.84K | 6pps | 3.34MB | 415.39MB |
| eth1 | 1:1181 | user | -3386852 | 71107 | 10.00K | 160.00K | 42.86K | 53.49K | 14pps | 2.04MB | 113.31MB |
| eth1 | 1:1183 | user | 3995074 | 109904 | 10.00K | 100.00K | 7.13K | 85 | 0 | 527.72KB | 4.20MB |
| eth1 | 1:1188 | user | -1987657 | -47316 | 10.00K | 100.00K | 16.41K | 14.29K | 1pps | 711.92KB | 27.59MB |
| eth1 | 1:1196 | user | 2049693 | 105710 | 10.00K | 100.00K | 14.99K | 2.85K | 5pps | 777.70KB | 22.98MB |
| eth1 | 1:1198 | user | -2280569 | 12619 | 10.00K | 320.00K | 112.02K | 144.79K | 24pps | 4.02MB | 84.00MB |
| eth1 | 1:1200 | user | 3995074 | 109904 | 10.00K | 100.00K | 408 | 169 | 0 | 23.20KB | 114.68MB |
| eth1 | 1:1223 | user | 2292173 | 89981 | 10.00K | 100.00K | 45.98K | 1.78K | 7pps | 581.34KB | 9.37MB |
| eth1 | 1:1230 | user | -309024 | 106234 | 10.00K | 100.00K | 16.49K | 16.99K | 14pps | 797.56KB | 18.20MB |
| eth1 | 1:1231 | user | -1880878 | 80416 | 10.00K | 100.00K | 16.58K | 4.04K | 2pps | 1.15MB | 39.93MB |
| eth1 | 1:3 | local | 27375 | 14296 | 1.40M | 1.40M | 2.09K | 2.10K | 0 | 10.19KB | 1011.70KB |

gdzie :

Rate, Ceil – zdefiniowane przepustowości klas: gwarantowana i maksymalna*Current Speed [bit/s]* – bieżąca prędkość klasy w bitach na sek.*Current Speed [pkt/s]* – bieżąca prędkość klasy w pakietach na sek.*Cumulated Send* – transfer klasy w bajtach zliczony od momentu uruchomienia monitora*Total Send* – transfer klasy w bajtach zliczony od ostatniego restartu shaper'a

Serwer ISP – Monitorowanie parametrów systemu

1. Informacje o systemie dostępne ze strony www :

System Information: localhost.localdomain

| System Vital | |
|--------------------|-----------------------------|
| Canonical Hostname | localhost.localdomain |
| Listening IP | 192.168.1.2 |
| Kernel Version | 2.6.18.6-p4 |
| Distro Name | Debian 3.1 |
| Uptime | 10 days 16 hours 21 minutes |
| Current Users | 2 |
| Load Averages | 0.22 0.09 0.02 4.3% |

| Network Usage | | | |
|---------------|-----------|-----------|----------|
| Device | Received | Sent | Err/Drop |
| eth0 | 62.35 MB | 3.93 GB | 0/0 |
| eth1 | 731.19 MB | 3.35 GB | 0/0 |
| eth2 | 1.47 GB | 2.86 GB | 0/0 |
| eth3 | 0.00 KB | 0.00 KB | 0/0 |
| lo | 495.49 MB | 495.49 MB | 0/0 |
| teql0 | 0.00 KB | 0.00 KB | 0/0 |
| irmq0 | 564.74 MB | 559.12 MB | 0/0 |
| irmq1 | 1.51 GB | 991.46 MB | 0/0 |
| eth4 | 0.00 KB | 0.00 KB | 0/0 |

| Hardware Information | |
|----------------------|--|
| Processors | 1 |
| Model | Intel(R) Celeron(R) CPU 2.80GHz |
| CPU Speed | 2.8 GHz |
| Cache Size | 256.00 KB |
| System Bogomips | 5604.99 |
| PCI Devices | - 0106: Intel Corp.: Unknown device 27c1 - 0403: Intel Corp.: Unknown device 27d8 - (3x) Ethernet controller: 3Com Corporation 3c905C-TX/TX-M [Tornado] - Ethernet controller: Intel Corp.: Unknown device 27dc - FireWire - Host bridge: Intel Corp.: Unknown device 2770 - IDE interface: Intel Corp.: Unknown device 27df - ISA bridge: Intel Corp.: Unknown device 27b8 - PCI bridge: Intel Corp. 82801 PCI Bridge - PCI bridge: Intel Corp.: Unknown device 27d0 - PCI bridge: Intel Corp.: Unknown device 27d4 - PCI bridge: Intel Corp.: Unknown device 27d6 - PCI bridge: Intel Corp.: Unknown device 27e0 - PCI bridge: Intel Corp.: Unknown device 27e2 - SMBus: Intel Corp.: Unknown device 27da - USB Controller: Intel Corp.: Unknown device 27c8 - USB Controller: Intel Corp.: Unknown device 27c9 - USB Controller: Intel Corp.: Unknown device 27ca - USB Controller: Intel Corp.: Unknown device 27cb - USB Controller: Intel Corp.: Unknown device 27cc - VGA compatible controller: Intel Corp.: Unknown device 2772 |
| IDE Devices | - hdb: LITE-ON DVD SHD-16P1S |
| SCSI Devices | - ATA WDC WD800JD-00MS (Direct-Access) - ATA WDC WD800JD-75MS (Direct-Access) |
| USB Devices | none |

| Memory Usage | | | | |
|-------------------------|------------------|-----------|-----------|-----------|
| Type | Percent Capacity | Free | Used | Size |
| Physical Memory | 99% | 10.11 MB | 874.38 MB | 884.50 MB |
| - Kernel + applications | 51% | | 453.04 MB | |
| - Buffers | 13% | | 112.58 MB | |
| - Cached | 35% | | 308.76 MB | |
| Disk Swap | 0% | 954.42 MB | 2.54 MB | 956.96 MB |

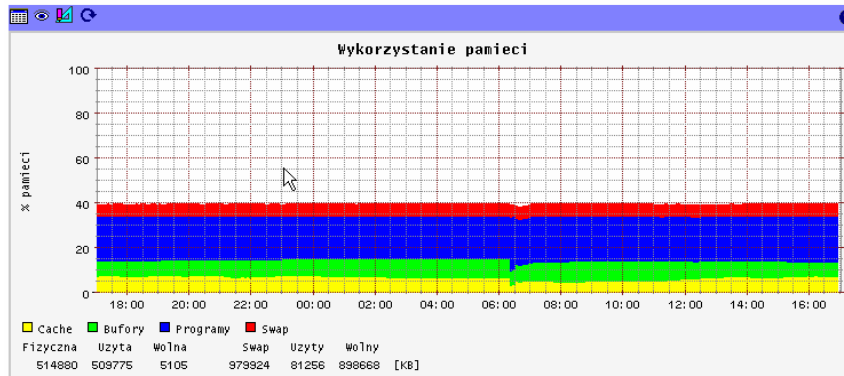
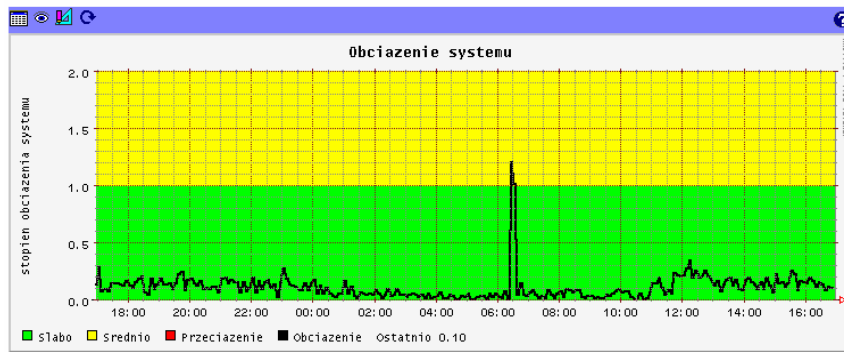
| Mounted Filesystems | | | | | | |
|---------------------|----------|-----------|------------------|-----------|----------|-----------|
| Mount | Type | Partition | Percent Capacity | Free | Used | Size |
| / | ext3 | /dev/sda1 | 63% | 1.44 GB | 2.91 GB | 4.58 GB |
| /var/spool/squid1 | reiserfs | /dev/sda6 | 24% (8%) | 14.15 GB | 4.48 GB | 18.63 GB |
| /var | ext3 | /dev/sda7 | 17% (1%) | 14.22 GB | 3.18 GB | 18.34 GB |
| /home | ext3 | /dev/sda8 | 0% | 29.52 GB | 79.04 MB | 31.18 GB |
| /var/spool/squid2 | reiserfs | /dev/sdb5 | 24% | 14.15 GB | 4.48 GB | 18.63 GB |
| /dev | tmpfs | tmpfs | 25% (1%) | 7.46 MB | 2.54 MB | 10.00 MB |
| /dev/shm | tmpfs | tmpfs | 0% (2%) | 442.25 MB | 0.00 KB | 442.25 MB |
| Totals : | | | | 73.49 GB | 15.13 GB | 91.37 GB |

| Temperature | | |
|-------------|-------|-------|
| Label | Value | Limit |
| Board | 33°C | 35°C |
| CPU | 37°C | 50°C |
| Remote | 30°C | 35°C |

| Voltage | | | |
|---------|----------|----------|----------|
| Label | Value | Min | Max |
| V1.5 | +1.55 V | +1.42 V | +1.58 V |
| VCore | +1.35 V | +1.76 V | +1.95 V |
| V3.3 | +3.33 V | +3.13 V | +3.47 V |
| V5 | +5.08 V | +4.74 V | +5.26 V |
| V12 | +12.06 V | +11.38 V | +12.62 V |

| Fans | | | |
|---------|----------|----------|-----|
| Label | Value | Min | Div |
| CPU_Fan | 1090 RPM | 4000 RPM | 0 |
| fan2 | 0 RPM | 0 RPM | 0 |
| fan3 | 0 RPM | 0 RPM | 0 |
| fan4 | 0 RPM | 0 RPM | 0 |

2. Informacje o obciążeniu systemu dostępne ze strony www - Istat:



3. Informacje o parametrach systemu dostępne w trybie konsoli

monitor parametrów sprzętowych :

```
netlan-d:/# sensors

lm85-i2c-0-2e
Adapter: SMBus I801 adapter at 2000
V1.5:      +1.55 V (min = +1.42 V, max = +1.58 V)
VCore:    +1.35 V (min = +1.76 V, max = +1.95 V)  ALARM
V3.3:     +3.33 V (min = +3.13 V, max = +3.47 V)
V5:       +5.08 V (min = +4.74 V, max = +5.26 V)
V12:     +12.06 V (min = +11.38 V, max = +12.62 V)
CPU_Fan:  1089 RPM (min = 4000 RPM)  ALARM
fan2:     0 RPM (min = 0 RPM)
fan3:     0 RPM (min = 0 RPM)
fan4:     0 RPM (min = 0 RPM)
CPU:      +35°C (low = +10°C, high = +50°C)
Board:    +33°C (low = +10°C, high = +35°C)
Remote:   +30°C (low = +10°C, high = +35°C)
CPU_PWM:  51
Fan2_PWM: 76
Fan3_PWM: 76
vid:     +1.850 V (VRM Version 9.1)
```

monitor systemu i procesów:

```
netlan-g:/# atop
ATOP - netlan-g 01/15/2007 16:56:50 10 seconds elapsed
PRC | sys 350 ms | user 170 ms | #thr 70 | #exits 0 | #zombie 0 |
CPU | sys 2% | user 2% | irq 7% | idle 89% | wait 0% |
MEM | tot 884.5M | free 8.8M | cache 340.7M | buff 107.2M | slab 139.2M |
SWP | tot 957.0M | free 957.0M | vmcom 316.2M | swin 0 | swout 0 |
DSK | sdb busy 0% | read 2 | write 12 | avio 0 ms |
DSK | sda busy 0% | read 0 | write 40 | avio 0 ms |
NET | transport tcpip 2058 | tcpi 2121 | udpi 32 | udpo 32 |
NET | network ipi 7887 | ipo 7537 | ipfrw 4828 | deliv 2715 |
NET | dev imq1 pcki 4064 | pcko 3771 | in 582K | out 558K |
NET | dev eth1 pcki 4070 | pcko 3192 | in 647K | out 2407K |
NET | dev imq0 pcki 3178 | pcko 3174 | in 2395K | out 2391K |
NET | dev eth0 pcki 2514 | pcko 3143 | in 967K | out 451K |
NET | dev eth2 pcki 1227 | pcko 860 | in 1517K | out 154K |
NET | dev lo pcki 82 | pcko 82 | in 7K | out 7K |
```

Serwer ISP – Logowanie i analiza połączeń użytkowników

Mechanizmy logowania umożliwiają m.in.

1. Logowanie wszystkich połączeń nawiązywanych przez użytkowników sieci. Może to być wykorzystane np. w celu ustalenia adresu ip z którego było nawiązane połączenie do innej maszyny w Internecie, co do którego istnieje podejrzenie że mogło być złamaniem prawa. Można sobie wyobrazić sytuacje w której organa ścigania zgłaszają się do operatora sieci celem wskazania użytkownika który danego dnia próbował wykonać transakcję przez internetowy serwis aukcyjny Allegro.

```
Jan 26 15:26:13 router2 kernel: !NEWTCP :IN=eth1 OUT= MAC=00:04:75:a0:18:70:00:80:c6:e8:6a:29:08:00 SRC=192.168.0.130 DST=91.121.14.7 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=2727 DF PROTO=TCP SPT=3460 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0
Jan 26 15:26:13 router2 kernel: !NEWTCP :IN=eth1 OUT= MAC=00:04:75:a0:18:70:00:0d:f3:03:58:6d:08:00 SRC=192.168.0.183 DST=66.234.224.3 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=49769 DF PROTO=TCP SPT=2138 DPT=25 WINDOW=65535 RES=0x00 SYN URGP=0
Jan 26 15:26:13 router2 kernel: !NEWTCP :IN=eth1 OUT= MAC=00:04:75:a0:18:70:00:80:c6:e8:a4:11:08:00 SRC=192.168.0.236 DST=62.121.83.61 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=38024 DF PROTO=TCP SPT=1253 DPT=4662 WINDOW=16384 RES=0x00 SYN URGP=0
Jan 26 15:26:13 router2 kernel: !NEWTCP :IN=eth1 OUT= MAC=00:04:75:a0:18:70:00:80:c6:e8:9b:93:08:00 SRC=192.168.0.122 DST=212.139.181.64 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=6876 DF PROTO=TCP SPT=1750 DPT=9716 WINDOW=16384 RES=0x00 SYN URGP=0
Jan 26 15:26:14 router2 kernel: !NEWTCP :IN=eth1 OUT= MAC=00:04:75:a0:18:70:00:11:95:51:6d:7e:08:00 SRC=192.168.0.223 DST=207.229.11.58 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=21785 DF PROTO=TCP SPT=4208 DPT=25 WINDOW=16384 RES=0x00 SYN URGP=0
```

2. Podgląd bieżących połączeń użytkownika do celów statystycznych i diagnostycznych.

Bieżące połączenia użytkownika 192.168.10.147 sklasyfikowane przez filtr 17 jako połączenia do sieci p2p torrent :

```
tcp 6 40 TIME_WAIT src=189.12.52.17 dst=84.40.157.22 sport=50402 dport=5147 packets=6 bytes=384 src=192.168.10.147 dst=189.12.52.17 sport=5147 dport=50402 packets=4 bytes=168 [ASSURED] mark=2 l7proto=bittorrent use=1
tcp 6 366409 ESTABLISHED src=192.168.10.147 dst=74.114.139.88 sport=4909 dport=12226 packets=6 bytes=520 src=74.114.139.88 dst=84.40.157.22 sport=12226 dport=4909 packets=1 bytes=48 [ASSURED] mark=2 l7proto=bittorrent use=1
tcp 6 282302 ESTABLISHED src=195.22.44.122 dst=84.40.157.22 sport=27288 dport=5147 packets=3 bytes=196 src=192.168.10.147 dst=195.22.44.122 sport=5147 dport=27288 packets=5 bytes=1976 [ASSURED] mark=2 l7proto=bittorrent use=1
tcp 6 33 SYN_SENT src=192.168.10.147 dst=83.9.159.82 sport=2989 dport=8122 packets=3 bytes=144 [UNREPLIED] src=83.9.159.82 dst=84.40.157.22 sport=8122 dport=2989 packets=0 bytes=0 mark=0 use=1
udp 17 62 src=192.168.10.147 dst=70.16.96.194 sport=5147 dport=34499 packets=3 bytes=374 src=70.16.96.194 dst=84.40.157.22 sport=34499 dport=5147 packets=2 bytes=260 [ASSURED] mark=2 l7proto=bittorrent use=1
```

Bieżące połączenia użytkownika 192.168.10.163 sklasyfikowane przez filtr 17 jako połączenia do sieci p2p edonkey :

```
tcp 6 116 TIME_WAIT src=213.76.183.87 dst=84.40.157.22 sport=28141 dport=5163 packets=8 bytes=522 src=192.168.10.163 dst=213.76.183.87 sport=5163 dport=28141 packets=6 bytes=507 [ASSURED] mark=2 l7proto=edonkey use=1
tcp 6 33 TIME_WAIT src=83.27.225.212 dst=84.40.157.22 sport=3080 dport=5163 packets=11 bytes=757 src=192.168.10.163 dst=83.27.225.212 sport=5163 dport=3080 packets=11 bytes=814 [ASSURED] mark=2 l7proto=edonkey use=1
tcp 6 59 TIME_WAIT src=192.168.10.163 dst=87.207.237.180 sport=1573 dport=4662 packets=9 bytes=656 src=87.207.237.180 dst=84.40.157.22 sport=4662 dport=1573 packets=8 bytes=569 [ASSURED] mark=2 l7proto=edonkey use=1
tcp 6 203292 ESTABLISHED src=192.168.10.163 dst=218.19.117.249 sport=5163 dport=50312 packets=2 bytes=82 [UNREPLIED] src=218.19.117.249 dst=84.40.157.22 sport=50312 dport=5163 packets=0 bytes=0 mark=0 use=1
tcp 6 16841 ESTABLISHED src=192.168.10.163 dst=81.210.76.30 sport=5163 dport=1843 packets=2 bytes=82 [UNREPLIED] src=81.210.76.30 dst=84.40.157.22 sport=1843 dport=5163 packets=0 bytes=0 mark=0 use=1
```

Bieżące połączenia http nawiązane poprzez serwer proxy

```
tcp 6 390103 ESTABLISHED src=192.168.10.1 dst=192.168.10.89 sport=8080 dport=1785 packets=1 bytes=1446 [UNREPLIED] src=192.168.10.89 dst=192.168.10.1 sport=1785 dport=8080 packets=0 bytes=0 mark=6 use=1
tcp 6 75 TIME_WAIT src=192.168.10.40 dst=38.99.76.170 sport=1574 dport=80 packets=6 bytes=610 src=192.168.10.1 dst=192.168.10.40 sport=8080 dport=1574 packets=5 bytes=778 [ASSURED] mark=6 use=1
tcp 6 49 TIME_WAIT src=83.12.77.163 dst=192.168.10.1 sport=60358 dport=80 packets=17 bytes=6315 src=192.168.10.1 dst=83.12.77.163 sport=80 dport=60358 packets=14 bytes=11621 [ASSURED] mark=0 l7proto=unknown use=1
tcp 6 204427 ESTABLISHED src=192.168.10.1 dst=192.168.10.114 sport=8080 dport=1712 packets=1 bytes=1452 [UNREPLIED] src=192.168.10.114 dst=192.168.10.1 sport=1712 dport=8080 packets=0 bytes=0 mark=6 use=1
tcp 6 297053 ESTABLISHED src=192.168.10.1 dst=192.168.10.181 sport=8080 dport=1388 packets=1 bytes=1452 [UNREPLIED] src=192.168.10.181 dst=192.168.10.1 sport=1388 dport=8080 packets=0 bytes=0 mark=6 use=1
```

3. Logowanie ruchu wskazującego na zawirusowanie systemu użytkownika

Zarejestrowane pakiety pochodzące od użytkownika 192.168.1.130 sklasyfikowane jako wirusy pocztowe

```
Jan 17 23:24:34 router2 kernel: !MAILSPAM :IN=eth1 OUT=eth2 SRC=192.168.1.130 DST=65.171.225.137 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=36681 DF PROTO=TCP SPT=3314 DPT=25 WINDOW=64240 RES=0x00 SYN URGP=0
Jan 17 23:25:34 router2 kernel: !MAILSPAM :IN=eth1 OUT=eth2 SRC=192.168.1.130 DST=12.151.32.16 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=38014 DF PROTO=TCP SPT=3560 DPT=25 WINDOW=64240 RES=0x00 SYN URGP=0
Jan 17 23:26:35 router2 kernel: !MAILSPAM :IN=eth1 OUT=eth2 SRC=192.168.1.130 DST=139.15.237.6 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=40067 DF PROTO=TCP SPT=3851 DPT=25 WINDOW=64240 RES=0x00 SYN URGP=0
Jan 17 23:28:35 router2 kernel: !MAILSPAM :IN=eth1 OUT=eth2 SRC=192.168.1.130 DST=216.236.131.172 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=44958 DF PROTO=TCP SPT=4415 DPT=25 WINDOW=64240 RES=0x00 SYN URGP=0
Jan 17 23:31:35 router2 kernel: !MAILSPAM :IN=eth1 OUT=eth2 SRC=192.168.1.130 DST=195.238.5.129 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=51627 DF PROTO=TCP SPT=1301 DPT=25 WINDOW=64240 RES=0x00 SYN URGP=0
```