

4. mājas darbs kursā Operētājsistēmas II

7. Tīkla plūsmu informācijas apkopošana un atskaites (munin, ntop), jādemonstrē lielākās atskaites.

MUNIN

Munin pēta tīkla datorus un atceras, ko tie darījuši. Visu iegūto informāciju tā attēlo grafiski, izmantojot web saskarsni. Uzsvars tiek likts uz “plug and play” iespējām. Pēc instalācijas daudzi no novērošanas spraudņiem, darbosies bez piepūles. Lietojot *munin*, jūs variet viegli novērot datoru, tīkla, atmiņas apgabalu tīklu, un, iespējams, arī programmu darbību. Tas ļauj viegli noteikt “kas šodien jauns”, kad rodas darbības traucējumi, kā arī vienkārši konstatēt, cik gudri Jūs rīkojieties ar ierobežotajiem resursiem.

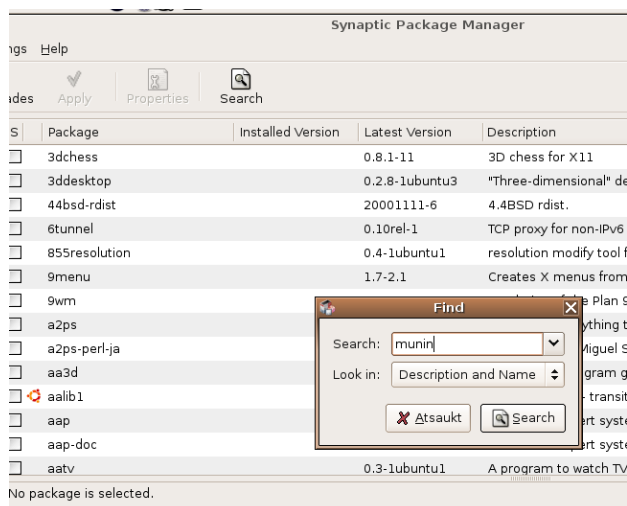
Munin lieto RRD rīku un uzrakstīts *Perl*. *Munin* izmanto servera/klienta arhitektūru, kur serveris regulāri pieslēdzas visiem klientiem un ievāc informāciju. Tad tas saglabā datus RRD failos, un pēc vajadzības atjauno grafikus. Viena no labākajām tā īpašībām ir jaunu spraudņu (grafu) izveidošanas vienkāršība.

munin (*munin* serveris)- programmas daļa, kas zīmē novērojumu grafikus
munin-node (*munin* klients)- munin klienta programma

Munin instalēšana

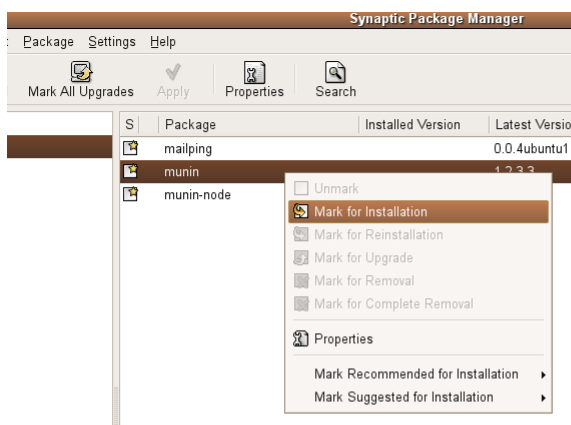
1. *Synaptic Manager*-ī jāatrod *munin*. Visvienkāršāk to izdarīt izmantojot *Search* pogu:

Klikšķinot uz *Search*, atveras *Find* logs, kurā jāieraksta *munin*:



Klikšķina uz *Search*, tiek atrastas vajadzīgās pakotnes.

Atzīmē instalācijai *munin* un *munin-node*:



4. *Apply* -> *Pielietot*
 Programma *munin* ir uzinstalēta.

Tagad mapē */etc/munin* atrodas šādi faili:

munin.conf munin-node.conf plugin-conf.d plugins templates

Mapē */var/www/munin* ir šādi faili:

definitions.html index.html localdomain logo.png style.css

***munin* konfigurācija**

Lai pievienotu jaunus klientus, jākonfigurē *munin.conf* failu:

1) Terminālī jāraksta

```
user@ubuntu:~$ sudo gedit /etc/munin/munin.conf
```

Atvērsies fails. Zem šīm rindiņām:

```
# a simple host tree
[localhost.localdomain]
  address 127.0.0.1
  use_node_name yes
```

ieraksta:

```
[<jaunā klienta identifikators>]
  address <klienta IP adrese>
  use_node_name yes
```

***munin-node* konfigurācija**

Lai, lietojot *munin*, novērotu klientu datorus, uz tiem jābūt uzinstalētam *munin-node*.
 Jākonfigurē *munin-node.conf* failu. Lai to izdarītu,

1) Terminālī raksta:

```
user@ubuntu:~$ sudo gedit /etc/munin/munin-node.conf
```

Atvērsies fails.

2) Atrod rindu:

```
allow ^127\.0\.0\.1$
```

Un zem tās ieraksta, servera IP adresi, tādā pašā formātā. Piemēram:

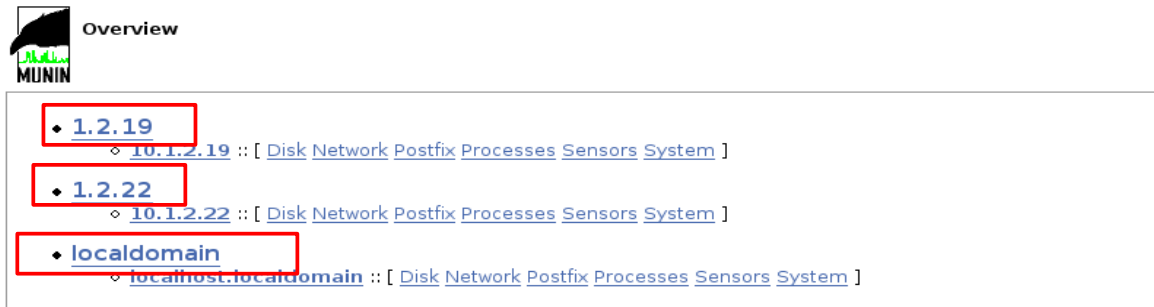
```
allow ^88\.110\.1\.154
```

Saglabā izmaiņas.

***munin* atskaites**

munin izveidotās atskaites grafiskā veidā var apskatīties atverot `/var/www/html` vai interneta pārlūkprogrammā, ierakstot `http://<IP adrese>/munin`. Tādā gadījumā abiem datoriem jābūt savā starpā savienotiem lokāli vai caur internetu. Lai apskatītos sava datora *munin* izveidotās atskaites: `http://localhost/munin`, jeb `http://127.0.0.1/munin`.

Piemēram, ja *munin* ir piesaistīti 2 *munin-node*, tad lapā būs redzama līdzīga situācija:



Overview

- **1.2.19**
 - [10.1.2.19](#) :: [[Disk](#) [Network](#) [Postfix](#) [Processes](#) [Sensors](#) [System](#)]
- **1.2.22**
 - [10.1.2.22](#) :: [[Disk](#) [Network](#) [Postfix](#) [Processes](#) [Sensors](#) [System](#)]
- **localhost**
 - [localhost.localdomain](#) :: [[Disk](#) [Network](#) [Postfix](#) [Processes](#) [Sensors](#) [System](#)]

kur `10.1.2.19`, `10.1.2.22`. un `localhost.localdomain` ir *munin* piesaistītās *munin-nodes*.

Nākamās sadaļas

[[Disk](#) [Network](#) [Postfix](#) [Processes](#) [Sensors](#) [System](#)]

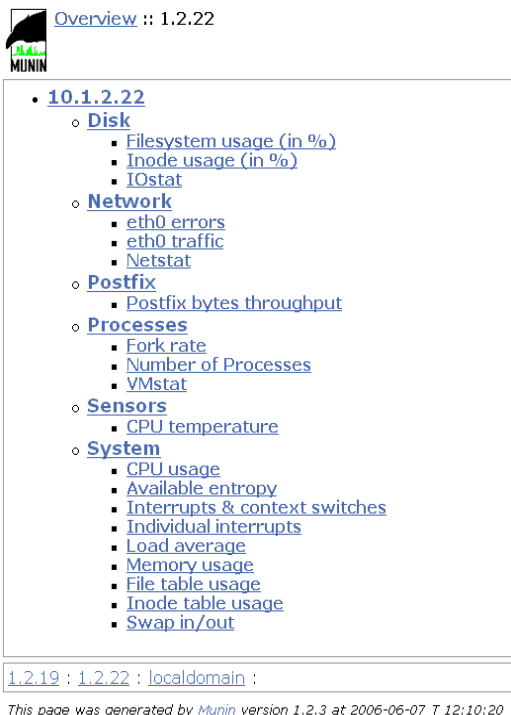
ir iespējas izvēlēties atsevišķi apskatīties atskaites par kādu noteiktu tēmu, piemēram, disku un tīklu.

Lai aplūkotu visas pieejamās atskaites, var izvēlēties novērojamo datoru identifikatorus:

• **1.2.22**

- [10.1.2.22](#) ::

tad atvērsies sadaļa ar pieejamajām atskaitēm, kas sagrupētas pēc tēmas:



Overview :: 1.2.22

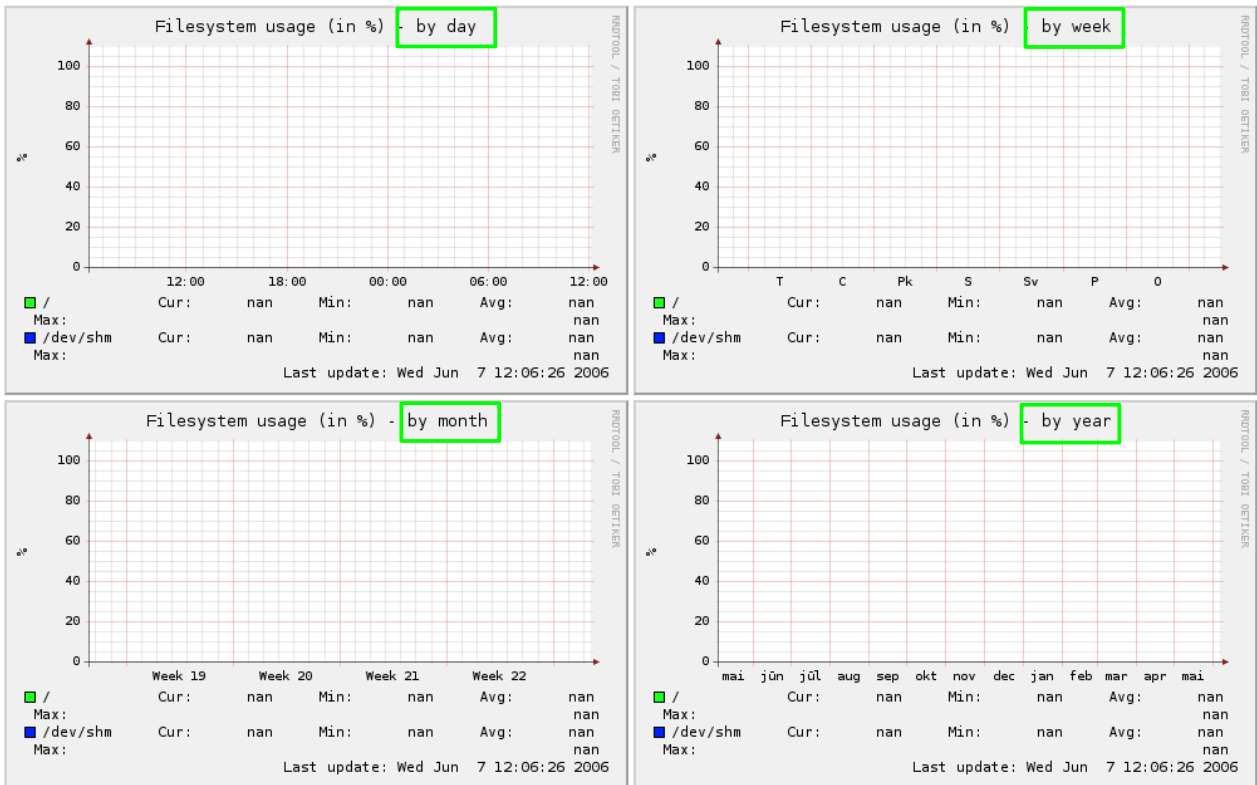
- **10.1.2.22**
 - **Disk**
 - [Filesystem usage \(in %\)](#)
 - [Inode usage \(in %\)](#)
 - [IOstat](#)
 - **Network**
 - [eth0 errors](#)
 - [eth0 traffic](#)
 - [Netstat](#)
 - **Postfix**
 - [Postfix bytes throughput](#)
 - **Processes**
 - [Fork rate](#)
 - [Number of Processes](#)
 - [VMstat](#)
 - **Sensors**
 - [CPU temperature](#)
 - **System**
 - [CPU usage](#)
 - [Available entropy](#)
 - [Interrupts & context switches](#)
 - [Individual interrupts](#)
 - [Load average](#)
 - [Memory usage](#)
 - [File table usage](#)
 - [Inode table usage](#)
 - [Swap in/out](#)

[1.2.19](#) : [1.2.22](#) : [localhost](#) :

This page was generated by [Munin](#) version 1.2.3 at 2006-06-07 T 12:10:20

Izvēloties kādu no šīm atskaitēm, *munin* sniegs par izvēlēto tēmu 4 atskaites: dienā, nedēļā, mēnesī

un gadā.



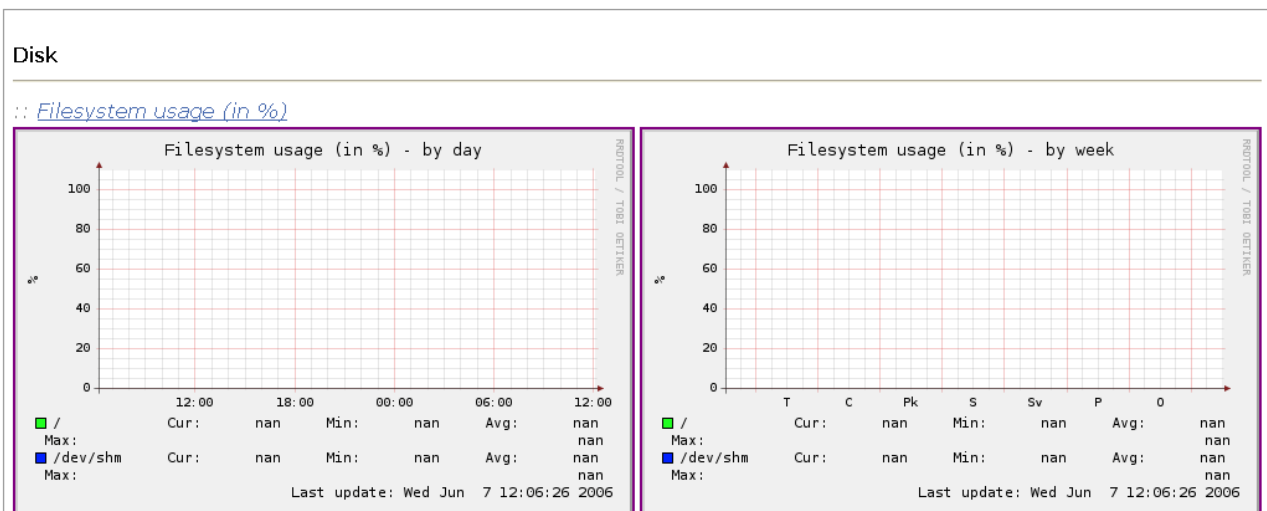
This graph shows disk usage on the machine.

Field	Internal name	Type	Warn	Crit	
/	_dev_sda1	gauge	92	98	/(ext3) -> /dev/sda1
/dev/shm	tmpfs_dev_shm	gauge	92	98	/dev/shm (tmpfs) -> tmpfs

Lai aplūkotu kopsavilkumu par visām atskaitēm, jāizvēlas datora adresi, mūsu gadījumā tā attiecīgi ir datora IP adrese.

- ◆ [1.2.22](#)
 - ◇ [10.1.2.22](#):

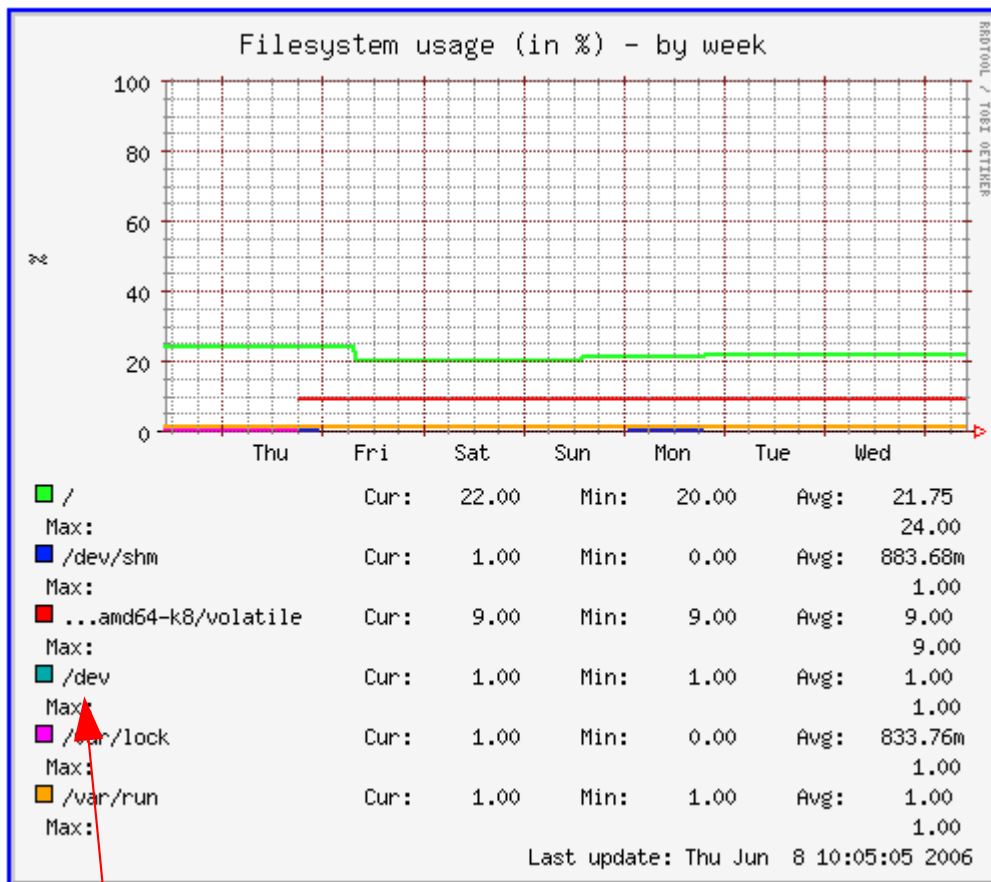
Tad tiks uzrādītas visas dienas un nedēļas atskaites.



Lielākās munin atskaites

Filesystem usage (in %)

Šī atskaite sniedz procentuālu informāciju par failu sistēmas izmantojumu, to attēlojot grafiku veidā.



Ar dažādajām krāsām tiek attēlotas mapes, kuru izmēru novēro *munin*.

Tiek dota arī informācija par:

1. Pašreiz izmantoto atmiņu - "Cur"
2. Minimālo izmantoto atmiņu - "Min"
3. Vidēji izmantoto atmiņu - "Avg"
4. Maksimāli izmantoto atmiņu - "Max"

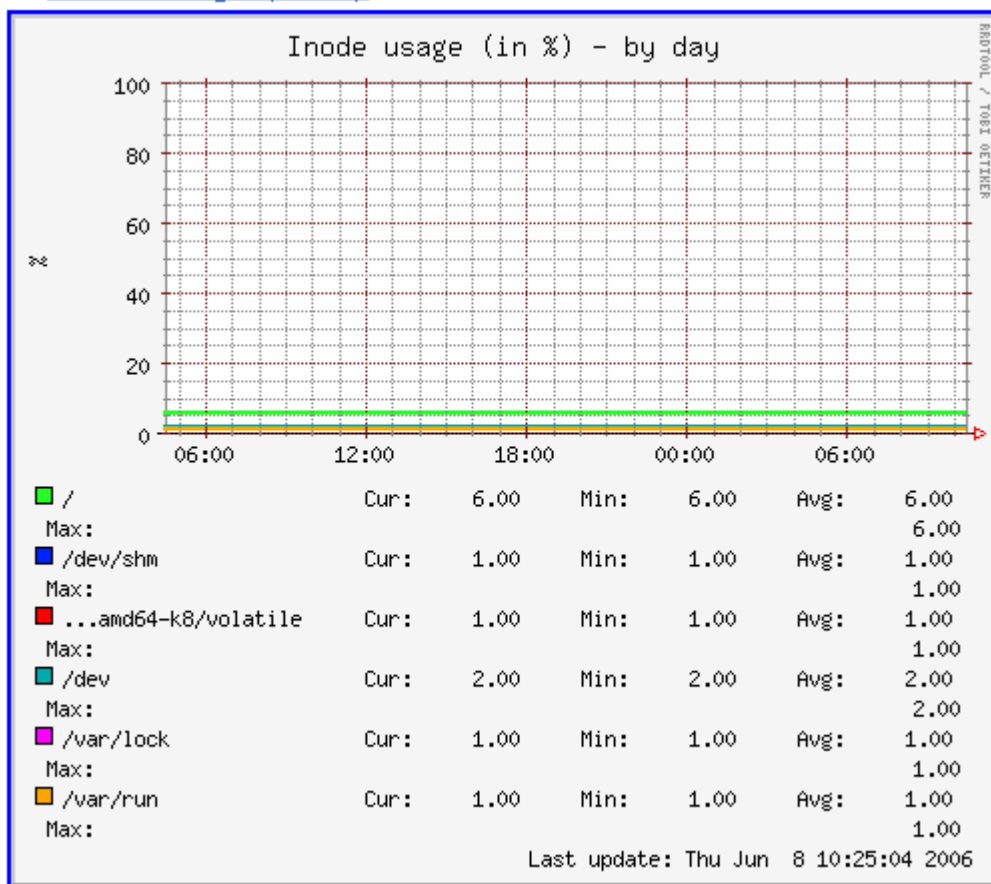
Uz X-ass atkarībā no izvēlētā grafika tiek rādīts pulksteņa laiks, nedēļas diena, mēnesis vai gads.

Šādu informāciju ir noderīgi iegūt, lai gadījumā, kad uz diska sāk pietrūkt vietas, lai uzzinātu, kas vietu ir aizņēmis. Var arī vienkārši aplūkot, cik daudz diska vietas tiek izmantots, kā arī sekot līdzi statistikai, kad diska vieta tiek patērēta visvairāk. Šāda informācija ir ļoti noderīga, ja tiek uzturēts kāds publisks failu serveris.

Inode usage (in %)

Šī atskaite sniedz procentālu informāciju par *inode* (failu sistēmas tabulas, kurās glabājas informācija/norādes par datu blokiem vai citām tabulām, kas glabā norādes uz datu blokiem).

:: *Inode usage (in %)*



Līdzīgi kā *filesystem* atskaitē arī šeit tiek rādīta informācija par:

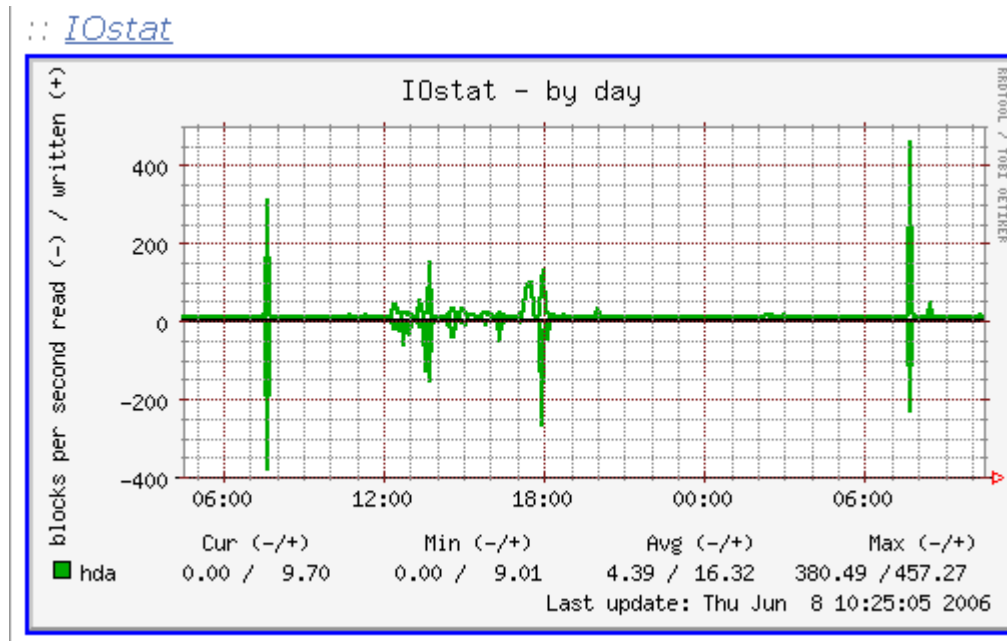
1. Pašreizējo inode lielumu - "Cur"
2. Minimālo inode lielumu - "Min"
3. Vidējo inode lielumu - "Avg"
4. Maksimālo inode lielumu - "Max"

Uz X-ass atkarībā no izvēlētā grafika tiek rādīts pulksteņa laiks, nedēļas diena, mēnesis vai gads.

Šāda informācija ir noderīga lai atrastu iespējamās problēmas failu sistēmā.

IOstat

Šī atskaite sniedz informāciju par cietā/o disku noslodzi – tiek parādīta statistika par to, cik datu bloki tiek ierakstīti sekundes laikā.



Grafiks, kas ir zem '0' vērtības attēlo lasīšanu, bet tas, kas ir virs '0' vērtības attēlo rakstīšanu.

Uz x ass atkarībā no izvēlētā grafika tiek rādīts pulksteņa laiks, nedēļas diena, mēnesis vai gads.

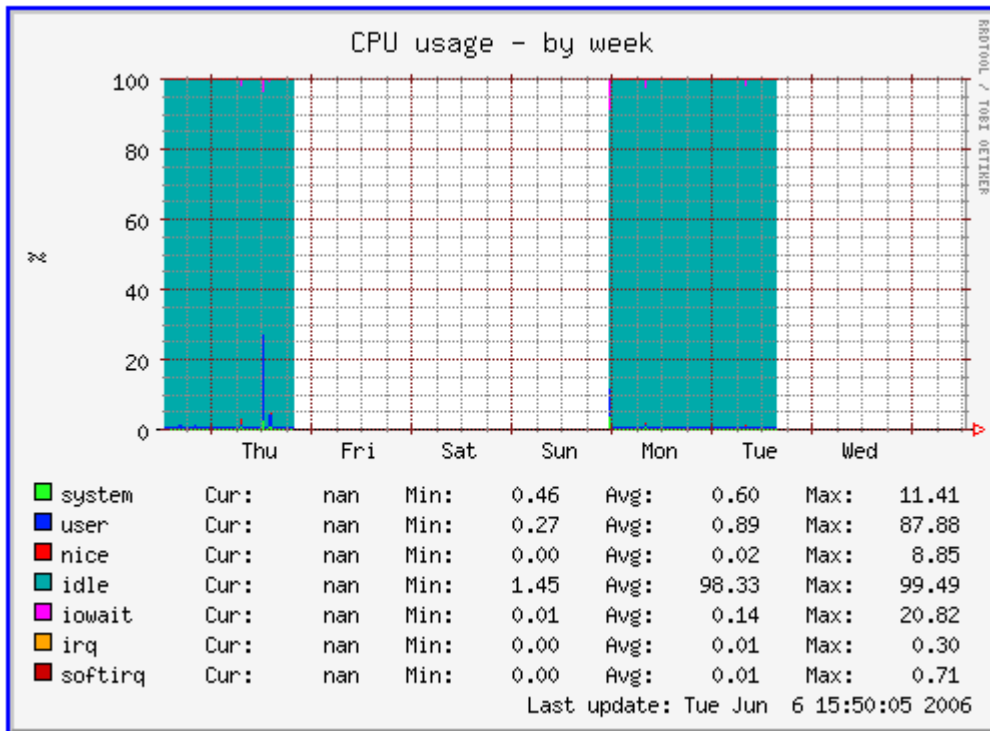
Tiek dota arī informācija par:

1. Pašreiz rakstīto bloku skaitu - "Cur (+)"
2. Pašreiz lasīto bloku skaitu - "Cur (-)"
3. Minimālo rakstīto bloku skaitu - "Min (+)"
4. Minimālo lasīto bloku skaitu - "Min (-)"
5. Vidēji rakstīto bloku skaitu - "Avg (+)"
6. Vidēji lasīto bloku skaitu - "Avg (-)"
7. Maksimāli rakstīto bloku skaitu - "Max (+)"
8. Maksimāli lasīto bloku skaitu - "Max (-)"

Apakšā parādās fiziskās ierīces kādas ir piemontētas. Piemēram, augstāk redzamajā grafikā ir piemontēts tikai 1 IDE's disks. Ja datoram tiktu pieslēgta USB zibatmiņa, tad sarakstā parādītos jauns disks - "sda", kā arī jauna sadaļa - "Total" kur tiktu rādīts kopējais ierakstīto bloku skaits abās atmiņas ierīcēs.

CPU usage

Šī atskaite sniedz informāciju par datora procesora noslodzi.



Tiek attēloti dažāda tipa procesi, kas noslogojuši procesoru.

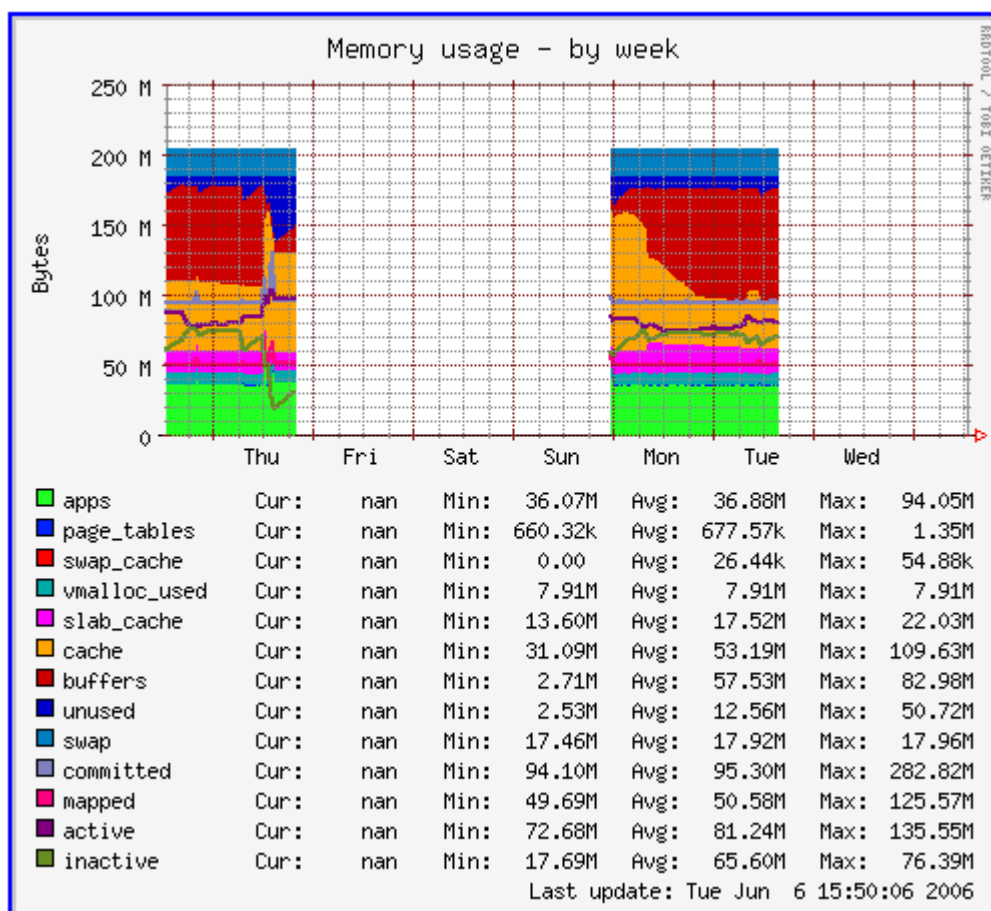
Apskatītie procesi ir:

1. System – sistēmas procesi
2. User – lietotāja aplikācijas
3. Idle – laiks kurā sistēma ir gatava darbam, bet neizpilda nekādus procesus, un tā kā procesors nevar vienkārši atslēgties, tad, kad nedara neko lietderīgu, tad, kā augstāk redzamams grafikā, šo laiku aizņem “dīklaiks”.
4. Iowait – ievada/izvada aktivitāte
5. Nice – procesu skaits, kuru prioritātes ir atšķirīgas no normālās
6. IRQ – pārtraukumu skaits
7. SoftIRQ – programmatūriskie pārtraukumi

Šāds grafiks ir noderīgs, lai atklātu iespējamus iemeslus, kādēļ ir samazinājusies datora ātrdarbība, piemēram, vai vainīgi ir sistēmas procesi vai lietotāja procesi.

Memory usage

Šī atskaite sniedz informāciju par datora atmiņas izmantošanu.



Svarīgākās sadaļas ir:

1. apps – atmiņa, kuru izmanto aplikācijas
2. swap – uz diska rezervētā vieta, kas papildina operatīvo atmiņu
3. committed – cik liela vieta ir rezervēta
4. unused – cik liela vieta netiek izmantota
5. active – cik liela vieta tiek izmantota

Uz vertikālās ass tiek attēlots atmiņas daudzums, bet uz horizontālās atkarībā no izvēlētā grafika tiek rādīts pulksteņa laiks, nedēļas diena, mēnesis vai gads.

Līdzīgi kā informāciju par CPU izmantošanu, arī šo var izmantot, lai atrastu iespējamās problēmas datora ātrdarbības samazināšanās gadījumā.

NTOP

ntop ir web balstīta novērošanas un datu plūsmas mērītājprogramma. Tā ļauj lietotājiem sekot līdzi svarīgiem tīkla notikumiem, ieskaitot datu plūsmas raksturlielumus, tīkla izmantošanu, tīkla protokolu lietojumu, un pārslodzes novērošanu. *ntop* paplašināmība ar dinamiski ielādējamām programmu komponentēm (spraudņiem) tīklu administratoriem dod iespēju padarīt to sev noderīgāku. Pie tam, drošības sistēmu defektu atrašanas iespējas ļauj *ntop* uziet potenciāli bīstamus datu pārraides apstākļus, tas ļauj dinamiski un autonomi piemērot tīkla konfigurāciju, lai risinātu novērotās problēmas.

ntop veic šādus uzdevumus:

- vienkārša datu plūsmas analīze;
- tīkla plūsmas sepecifikācija un mērīšana;

ntop ir iebūvēts HTTP serveris, lai vizualizētu datu plūsmu.

ntop instalēšana

Terminālī jāraksta sekojošas komandas:

```
wget http://http.us.debian.org/debian/pool/main/n/ntop/ntop_3.0-5_i386.deb
```

```
sudo apt-get install libpcap0.7
```

```
sudo dpkg -i ntop_3.0-5_i386.deb
```

```
sudo chmod -R 777 /var/lib/ntop
```

```
sudo ntop
```



Jāievada vismaz 5 simbolus gara parole.

ntop atskaites

Lai aplūkotu *ntop* atskaites, jāatver kāda interneta pārlūkprogramma un adreses laukā jāieraksta: *http://localhost:3000*, jeb *http://127.0.0.1:3000*.

Ja *ntop* atskaites vēlas aplūkot no kāda cita datora, tad var rakstīt *http://<datora IP adrese>:3000*. Tādā gadījumā abiem datoriem jābūt savā starpā savienotiem lokāli vai caur internetu.

Piemēram, ja atveram *http://localhost:3000* tiek atvērta *ntop* sākuklapa: ***Lielākās ntop atskaites***

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#) | [All Protocols](#) | [Local IP](#) | [FC](#) | [SCSI](#) | [Admin](#) | (C) 1998-2004 - L. Deri
 About: [What's ntop?](#) | [Configuration](#) | [Credits](#) | [Man Page](#) |  

Welcome to ntop!

ntop shows the current network usage. It displays a list of hosts that are currently using the network and reports information concerning the IP (Internet Protocol) and Fibre Channel (FC) traffic generated by each host. The traffic is sorted according to host and protocol. Protocols (user configurable) include:

- ◆ TCP/UDP/ICMP
- ◆ (R)ARP
- ◆ IPX
- ◆ DLC
- ◆ Decnet
- ◆ AppleTalk
- ◆ Netbios
- ◆ TCP/UDP
 - FTP
 - HTTP
 - DNS
 - Telnet
 - SMTP/POP/IMAP
 - SNMP
 - NFS
 - X11
- ◆ Fibre Channel
 - Control Traffic - SW2,G53,ELS
 - SCSI



ntop's author strongly believes in [open source software](#) and encourages everyone to modify, improve and extend **ntop** in the interest of the whole Internet community according to the enclosed licence (see COPYING).

Problems, bugs, questions, desirable enhancements, source code contributions, etc., should be sent to the [mailing list](#).

For information on **ntop** and information privacy, see [this](#) page.

Šeit ir pieejams neliels apraksts par ntop programmu, kā arī par tās populārākajām iespējām.

Lapas augšpuse ir veidota, kā divu līmeņu izvēlne, kur augšējā izvēlnē ir galvenās sadaļas.

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#) | [All Protocols](#) | [Local IP](#) | [FC](#) | [SCSI](#) | [Admin](#) | (C) 1998-2004 - L. Deri
 About: [What's ntop?](#) | [Configuration](#) | [Credits](#) | [Man Page](#) |  

Welcome to ntop!

Un klikšķinot uz tām attiecīgi apakšējā izvēlnē parādās apakšizvēlnes. Piemēram, izvēloties IP: Summary:

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#) | [All Protocols](#) | [Local IP](#) | [FC](#) | [SCSI](#) | [Admin](#) | (C) 1998-2004 - L. Deri
 IP: [Traffic](#) | [Multicast](#) | [Domain](#) | [Distribution](#) | [Local » Local](#) | [Local » Remote](#) | [Remote » Local](#) | [Remote » Remote](#)

Kopsavilkumā varētu teikt, ka ntop piedāvā ļoti plašas iespējas tīkla analīzei un novērošanai, piedāvājot apskatīt gan vispārējas atskaites, gan ļoti detalizētas.

Lielākās ntop atskaites

Summary : Traffic

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#)
Summary: [Traffic](#) | [Hosts](#) | [Network Load](#) | [ASN](#)

Sadaļā “Summary” -> “Traffic” var aplūkot plašu vispārējo informāciju par tīkla plūsmu.

Global Traffic Statistics

Global Traffic Statistics								
Network Interface(s)	Name	Device	Type	Speed	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		1514	14	██████████	::0
Local Domain Name	localdomain							
Sampling Since	Thu Jun 8 20:08:27 2006 [2:07:58]							
Active End Nodes	454							

Šī sadaļa parāda informāciju par:

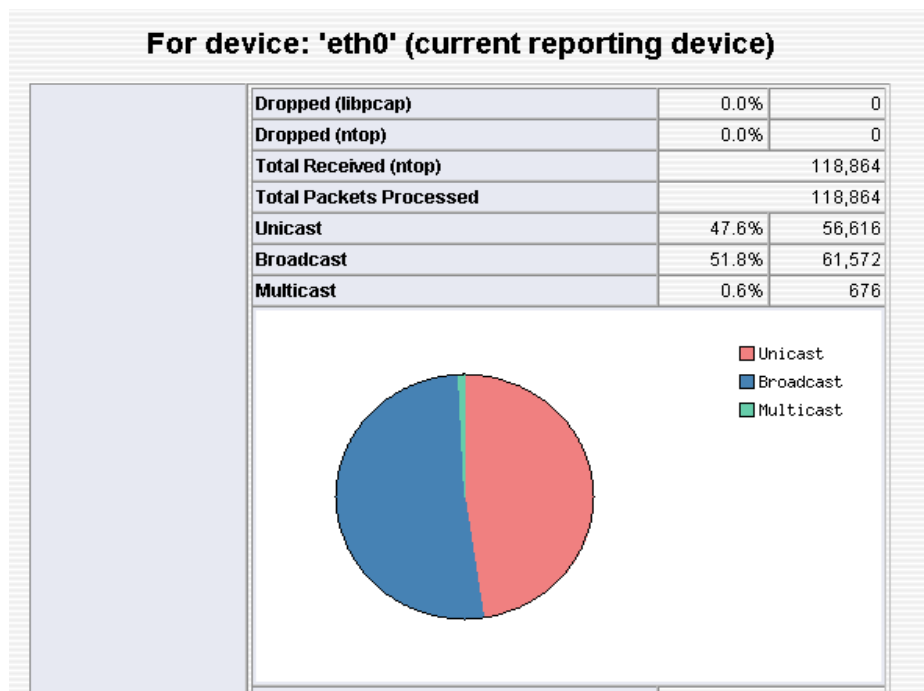
1. Network Interfaces – kādas tīkla ierīces ir pieslēgtas datoram
2. Name – ierīcei piešķirtais vārds
3. Device – ierīce
4. Type – kāda tipa tīklu atbalsta šī ierīce. ntop atbalsta šādas tīkla arhitektūras:
 - Ethernet (including 802.11Q)
 - Token Ring
 - PPP/PPPoE
 - Raw IP
 - FDDI
 - Loopback
 - FibreChannel

No augstāk redzamās atskaites var secināt, ka datoram ir pieslēgta 1 Ethernet tīkla karte

5. Speed – ātrums
6. MTU – lielākās pakas izmērs ko tīkla protokols spēj pārraidīt
7. Address – datora IP adrese
8. IPv6 – datora IP (sestās versijas) adrese

Tālāk lapā ir aplūkojama detalizētāka informācija par attiecīgajām tīkla ierīcēm.

Šī informācija ir pieejama gan skaitliski, kas palīdz sīkāk izanalizēt tīkla plūsmu, gan grafiski, izmantojot grafikus un diagrammas, kas palīdz vieglāk uztvert vispārējo situāciju.



Dažas interesantas atskaites:

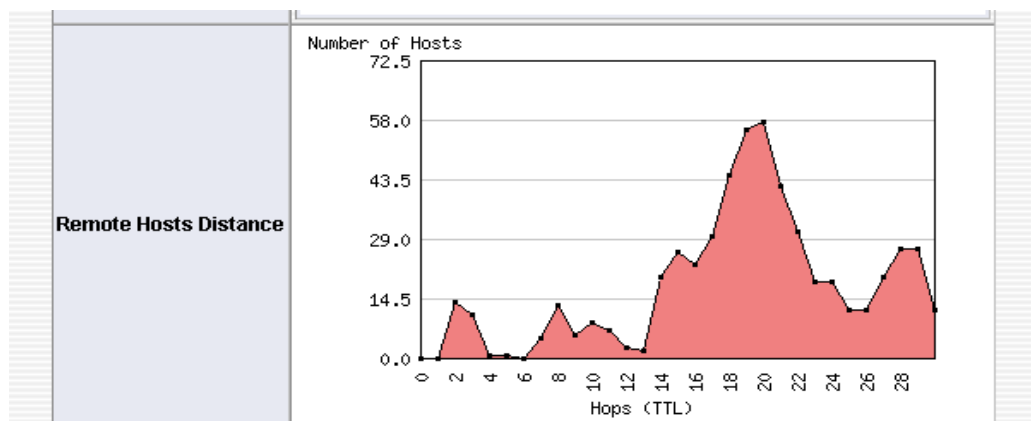
For device: 'eth0' (current reporting device)

Sadaļā “Packets” var aplūkot sūtīto un saņemto datu pakešu izmērus:

Packets	Shortest	42 bytes
	Average Size	123 bytes
	Longest	1,514 bytes

Tiek piedāvāts arī procentuāls uzskaitījums par to, cik lielas paketes ir tikušas nosūtītas/saņemtas.

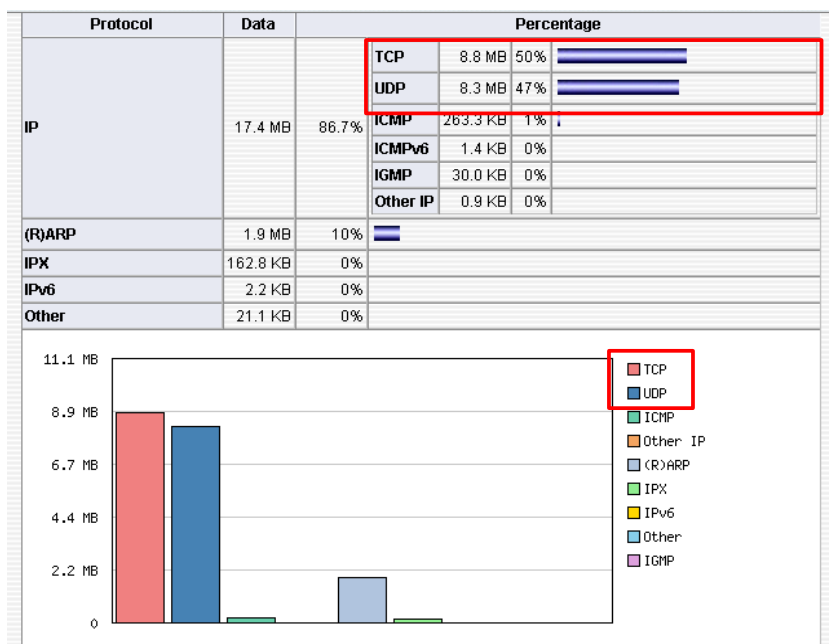
Samērā interesants ir arī grafiks, kas rāda, cik daudz “lēcienu” - *hops* ir izdarījušas sūtītās paketes. Pēc tā apmēram var nojaust attālumu līdz galapunktam.



Global Protocol Distribution

Šajā sadaļā ir pieejama informācija par to – kādi protokoli un cik daudz tie tiek izmantoti.

Piemēram, šajā grafikā ir redzams, ka pārsvarā ir izmantoti TCP un UDP protokoli, kas mūsdienās arī tiek izmantoti visplašāk



Global TCP/UDP Protocol Distribution

Šajā sadaļā var aplūkot, kurši no TCP / UDP protokoliem ir izmantots. *ntop* rāda statistiku ne tikai par pazīstamajiem protokoliem kā FTP (21. ports), HTTP (80. ports), bet arī Kazaa (1214. ports) un eDonkey(4661. Ports), kurus izmanto populāri failu apmaiņas tīkli.

TCP/UDP Protocol	Data	Percentage
FTP	29.5 KB	0%
HTTP	10.8 MB	43%
DNS	1.5 MB	6%
NBios-IP	4.5 MB	18%
Mail	1.4 KB	0%
DHCP-BOOTP	107.2 KB	0%
NFS/AFS	4.9 KB	0%
X11	0.3 KB	0%
SSH	0.1 KB	0%
Gnutella	0.2 KB	0%
Kazaa	1.6 KB	0%
eDonkey	154.1 KB	0%
messenger	1.5 KB	0%
Other TCP/UDP-based Protocols	7.5 MB	30%

No augstāk redzamās atskaites var sacināt, ka datora lietotājs visvairāk ir izmantojis HTTP protokolu – aplūkojis mājaslapas, kuras kopā ir aizņēmušas 10 MB.

IP Summary : Traffic

Interesanta sadaļa ir "IP Summary" -> "Traffic"



Šinī sadaļā parādās visa datu saņemtā un sūtītā datu plūsma.

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received														
Hosts: [All] [Local Only] [Remote Only]										Data: [All] [Sent Only] [Received Only]				
Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	X11	
ubuntu		19.0 MB 65.1 %	28.7 KB	10.7 MB	1.8 MB	0	1.9 KB	923	0	0	0	4.7 KB		
87.110.1.154		4.6 MB 15.7 %	28.7 KB	1.1 KB	0	0	1.6 KB	0	0	0	0	4.7 KB		
ns1.lainnet.lv		1.8 MB 6.1 %	0	0	1.8 MB	0	0	0	0	0	0	0	0	
80.233.186.114		168.7 KB 0.6 %	278	140	0	0	41.4 KB	0	0	0	0	0	0	
xp-c [NetBIOS]		149.6 KB 0.5 %	0	0	0	0	149.6 KB	0	0	0	0	0	0	
pavel [NetBIOS]		135.0 KB 0.5 %	0	0	0	0	134.8 KB	0	0	0	0	0	0	
80.233.197.114		131.4 KB 0.4 %	0	0	0	0	131.0 KB	0	0	0	0	0	0	
mel-33f94740975 [NetBIOS]		109.4 KB 0.4 %	0	0	0	0	109.4 KB	0	0	0	0	0	0	
ghost [NetBIOS]		101.1 KB 0.3 %	0	0	0	0	97.3 KB	124	0	0	0	0	0	
85.115.102.127		100.8 KB 0.3 %	0	0	0	0	0	0	0	0	0	0	0	
81.198.148.9		100.3 KB 0.3 %	0	0	0	0	0	0	0	0	0	0	0	

Atskaitē ir detalizēti parādīts:

1. Host – serveris, no kura/uz kuru tika raidīta informācija(dati)
2. Domain – valsts, kur atrodas *hosts* (tiek parādīta tad, ja *domains* satur tādu informāciju) tiek attēlota ar krāsainiem valstu karodziņiem
3. Data – informācijas(datu) daudzums, kas tika saņemts/sūtīts uz attiecīgo *hostu*
4. dažādi TCP protokoli

Pārskatāmībai atskaiti var sagrupēt pēc jebkuras no kolonnām.

Piemēram, augšējā attēlā atskaite ir sagrupēta pēc pārsūtīto datu daudzuma. Šādas atskaites ir ļoti noderīgas uzturot publiskus web un failu serverus. Un gadījumā, ja šiem serveriem uzbrūk, piemēram, pārsūtot paketes ar SYN karodziņu (pieprasot atvērt jaunu TCP konekciju), tad izmantojot šo rīku var atklāt uzbrucēju.

Šī atskaite arī detalizēti parāda informāciju par izmantotajiem protokoliem, kurus izmanto failu apmaiņas tīkli, tādi kā Gnutella, Kazaa, WinMX, DC++ un eDonkey. Iegūt informāciju par šādu tīklu izmantošanu būtu noderīgi, piemēram, ja šo tīklu izmantošana kādā uzņēmumā ir aizliegta, tad apskatot šo statistiku būtu ļoti viegli atrast "grēkāzi".

FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	X11	SSH	Gnutella	Kazaa	WinMX	DC++	eDonkey	Messenger
-----	------	-----	--------	----------	------	------------	------	------	---------	-----	-----	----------	-------	-------	------	---------	-----------

ntop piedāvā ne tikai vispārīgus pārskatus, bet arī detalizētu informāciju. Sadaļā "IP summary" -> "Traffic" var izvēlēties kādu noteiktu *hostu*, uz kura klikšķinot, parādās detalizēta informācija:

Hosts: [All] [Local Only] [Remote Only]

Host
ubuntu
ns1.lainnet.lv
llab.cs.fmf.lu.lv
komok [NetBIOS]
xp-c [NetBIOS]

Piemēram, papētot ns1.lainnet.lv *hostu* var iegūt šādu informāciju:

- Last MAC Address/Router – pēdējā MAC adrese caur kuru ir gājušas pakas no/uz izvēlēto *hostu*.
- IP TTL – caur cik serveriem/maršrutētājiem (*routers*) ir gājušas pakas
- Sent vs. Rcvd Data – sūtīto un saņemto datu attiecība
- Further Host Information – papildus informācija par hostu (informācija ko hosts par sevi dod)

Info about llab.cs.fmf.lu.lv

IP Address	195.13.158.143 [unicast]		
First/Last Seen	Fri Jun 9 09:22:00 2006 - Fri Jun 9 09:39:41 2006 [17:41]		
Domain	cs.fmf.lu.lv		
Last MAC Address/Router	00:0E:0C:69:CE:3D		
Origin AS	1		
Host Location	Remote (outside specified/local subnet)		
IP TTL (Time to Live)	56:56 [~8 hop(s)]		
Total Data Sent	103.1 KB/765 Pkts/0 Retran. Pkts [0%]		
Broadcast Pkts Sent	0 Pkts		
Data Sent Stats	Local 100 %		Rem 0 %
IP vs. Non-IP Sent	IP 100 %		Non-IP 0 %
Total Data Rcvd	216.1 KB/737 Pkts/0 Retran. Pkts [0%]		
Data Rcvd Stats	Local 100 %		Rem 0 %
IP vs. Non-IP Rcvd	IP 100 %		Non-IP 0 %
Sent vs. Rcvd Pkts	Sent 50.9 %		Rcvd 49.1 %
Sent vs. Rcvd Data	Sent 32.3 %		Rcvd 67.7 %
Further Host Information	[Whois]		

Host Traffic Stats

Time	Tot. Traffic Sent	% Traffic Sent	Tot. Traffic Rcvd	% Traffic Rcvd
9 AM	103.1 KB	100.0 %	216.1 KB	100.0 %
8 AM	0	0.0 %	0	0.0 %