

Optimisation del ancho de banda (Intro Monitoring)



Christian Benvenuti

christian.benvenuti@libero.it

La Paz, Bolivia, 4-9/5/2009



Monitoring

- Why does it mean “*monitoring the network*”?
- Why is it important to monitor the network?
- How can we monitor the network?
- What information do we need to better understand the status of the network? Do we only need to monitor the network?

Quick intro/review of basic Linux/Fedora concepts

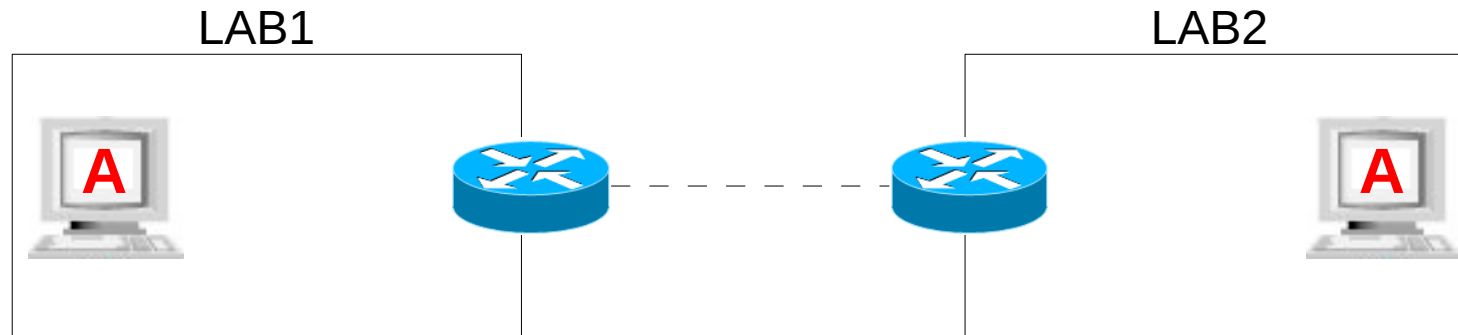
- Basic packages managements (*rpm, yum*)
 - Starting/stopping a system service
 - *service <service_name> status|start|stop*
 - Crond/Crontab
 - Logfiles (*syslog, /var/log/....*)
 - Configuration files (*/etc*)
 - Net utils (*ping, traceroute, ...*)
-
- SNMP
 - RRDtool (Round Robin Database tool)
 - Mysql

Monitoring - **tcpdump**

- Simple but powerful text-based packet analyzer
 - No TCP-only
 - Many options

Exercise - tcpdump

- User *umsa* can not ping from host A in LAB1 host B in a LAB2.



- The net-admin of LAB1 says he has configured everything in LAB1 to make this possible, therefore *umsa* suspects ... what?
 - How can user *umsa* use tcpdump to prove his theory?
 - OPTIONAL: how could user *umsa* send by email the proofs of his theory to the netadmin?

Monitoring - Wireshark

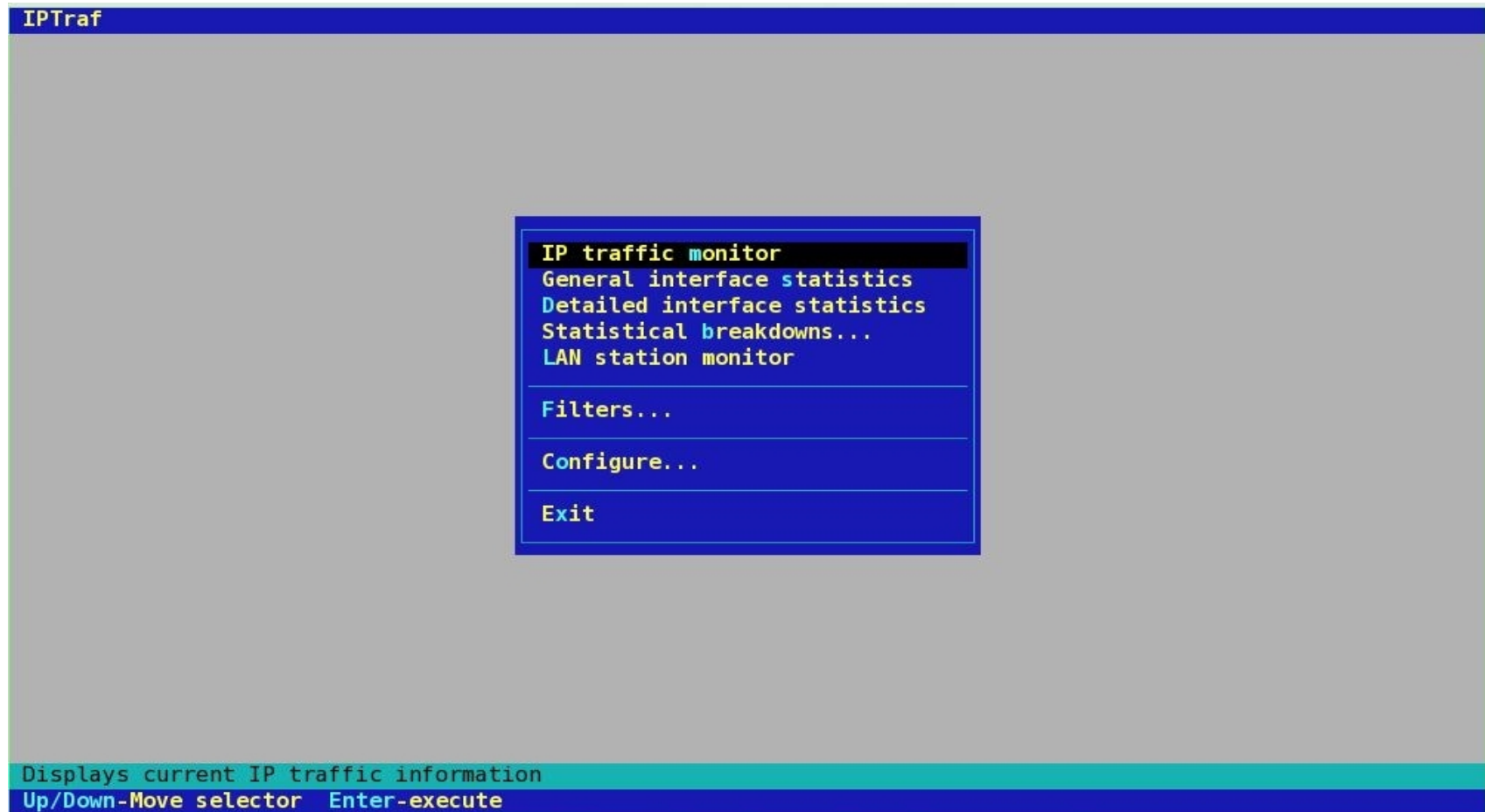
- The most powerful protocol analyzer
 - Powerfull
 - Actively maintained
 - Constantly updated

Exercise - Wireshark

- User *umsa* can not access the web with Firefox, but he can ping any remote host without problems.
 - What could be the problem?
 - User *umsa* suspects ... XXX ... and he decides to use Wireshark to prove it. HOW?

Monitoring - iptraf

- Simple and basic text-based monitoring tool
- It only shows the current state (no statistics/history)



The screenshot shows the IPtraf application window. The title bar is blue and contains the text "IPtraf". The main area is grey. A blue menu box is centered, containing the following text:

```
IP traffic monitor
General interface statistics
Detailed interface statistics
Statistical breakdowns...
LAN station monitor

Filters...

Configure...

Exit
```

At the bottom of the window, there is a cyan bar with the text "Displays current IP traffic information" and a blue bar with the text "Up/Down-Move selector Enter-execute".

Monitoring - Network Top (**NTOP**) (1/2)

- Mainly used to monitor the interfaces on the local host
- It can also monitor remote interfaces through the Netflow/sFlow protocols
- Powerful traffic classification
- Web interface
 - Embedded http/https server (ie, no need for Apache)
- Graphs based on RRDtool

Monitoring - Network TOP (NTOPT) (2/2)

- **Exercise 1**

- Check if it is already installed
 - *rpm -qi ntop*
- Install it if necessary
 - *yum install ntop*
- Identify the configuration file/s AND the init file
 - *rpm -ql ntop | grep etc*
- Start it

- **Exercise 2**

- Add all local devices to the configuration

- **Exercise 3**

- Connect with the browser to a remote *ntop* instance

The rest next week ...

Copyright



- This presentation is released under the Creative Common License:
 - Attribution, Noncommercial, Share Alike 2.5
 - (<http://creativecommons.org/licenses/by-nc-sa/2.5/>)
- Attribution
 - You must attribute the work in the manner specified by the author or licensor.
- Noncommercial.
 - You may not use this work for commercial purposes.
- Share Alike.
 - If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.