Optimisacion del ancho de banda (Intro Monitoring, 1st part)

Christian Benvenuti
christian.benvenuti@libero.it

Managua, Nicaragua, 31/8/9 - 11/9/9

UNAN-Managua

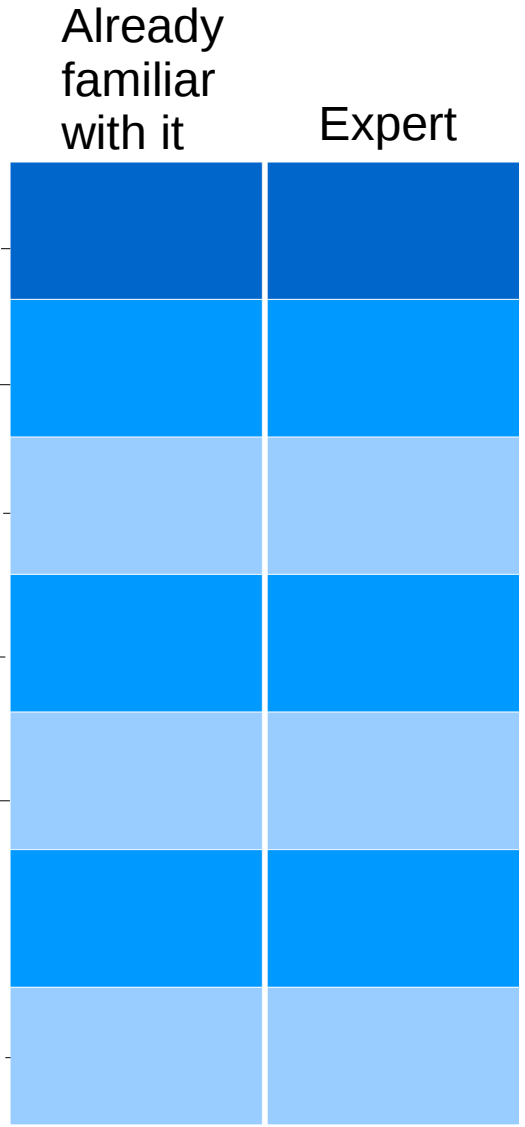
International Network INASP
for the Availability of Scientific Publications

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?

Monitoring

- Wireshark (http://www.wireshark.org)
  - tcpdump
- iptraf (*http://iptraf.seul.org/*)
- NTOP (*http://www.ntop.org*)
- MRTG (*http://oss.oetiker.ch/mrtg/*)
- NAGIOS (*http://www.nagios.org*)
- CACTI (*http://www.cacti.net*)
- ...
- netstat/lsoi/...



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*, ...)

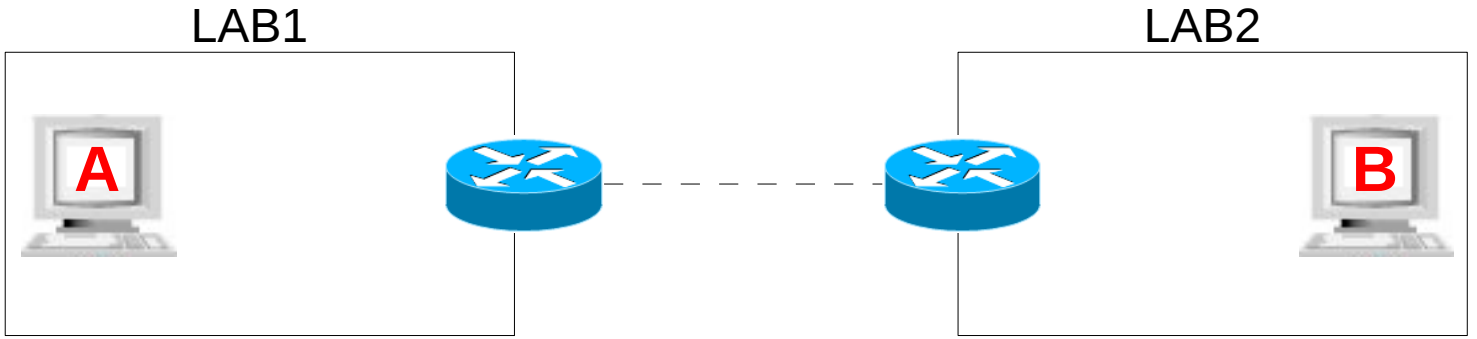
- SNMP
- RRDtool (Round Robin Database tool)
- Mysql

Monitoring - **tcpdump**

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

Exercize - tcpdump

- User *unan* can not ping from host A in LAB1 to host B in LAB2.



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

Monitoring - **Wireshark**

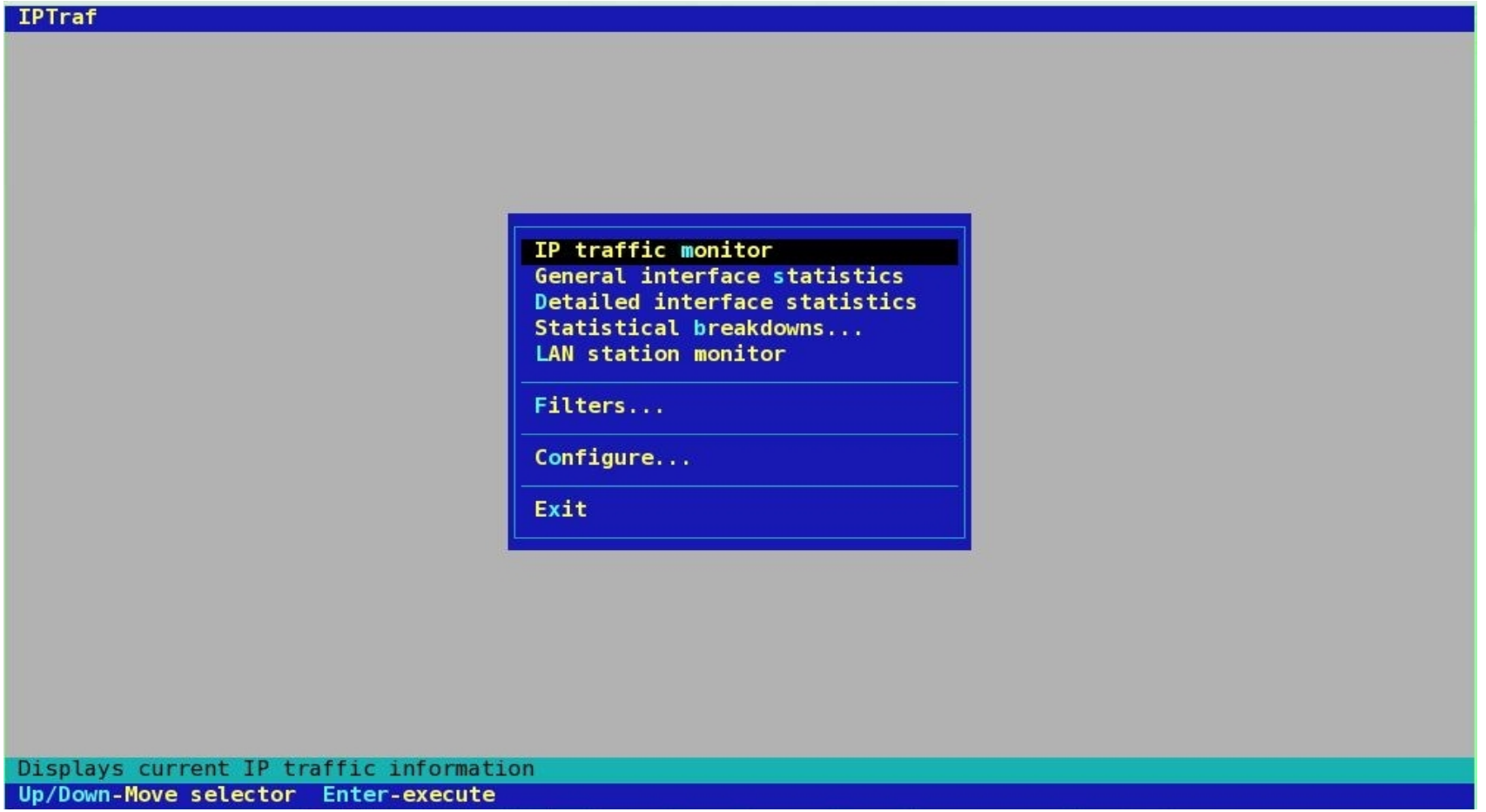
- The most powerful protocol analyzer
  - Powerfull
  - Actively maintained
  - Constantly updated

Exercize - wireshark

- User *unan* can not access the web with Firefox, but he can ping the gateway 192.168.1.1 and the local DNS X.Y.Z.K without problems.
  - What could be the problem?
  - User *unan* 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)



Monitoring - Network Top (**NTOP**) (1/3)

- 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 (**NTOP**) (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

Monitoring - Network TOP (**NTOP**) (3/3)

- **Exercise 3**
  - Connect with the browser to a remote *ntop* instance (for example the one running on the group's router or the lab's router).
    - Config users so that only admin can modify the config.
- **Exercise 4**
  - Why can't I see the MAC address of all hosts?
  - What can I say about those hosts that have the TX counters much bigger than the RX counters (and viceversa)?
  - Does NTOP run as a daemon?
  - How can I check what port does it listen to?

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.