Network Monitoring

Sebastian Büttrich, sebastian@less.dk

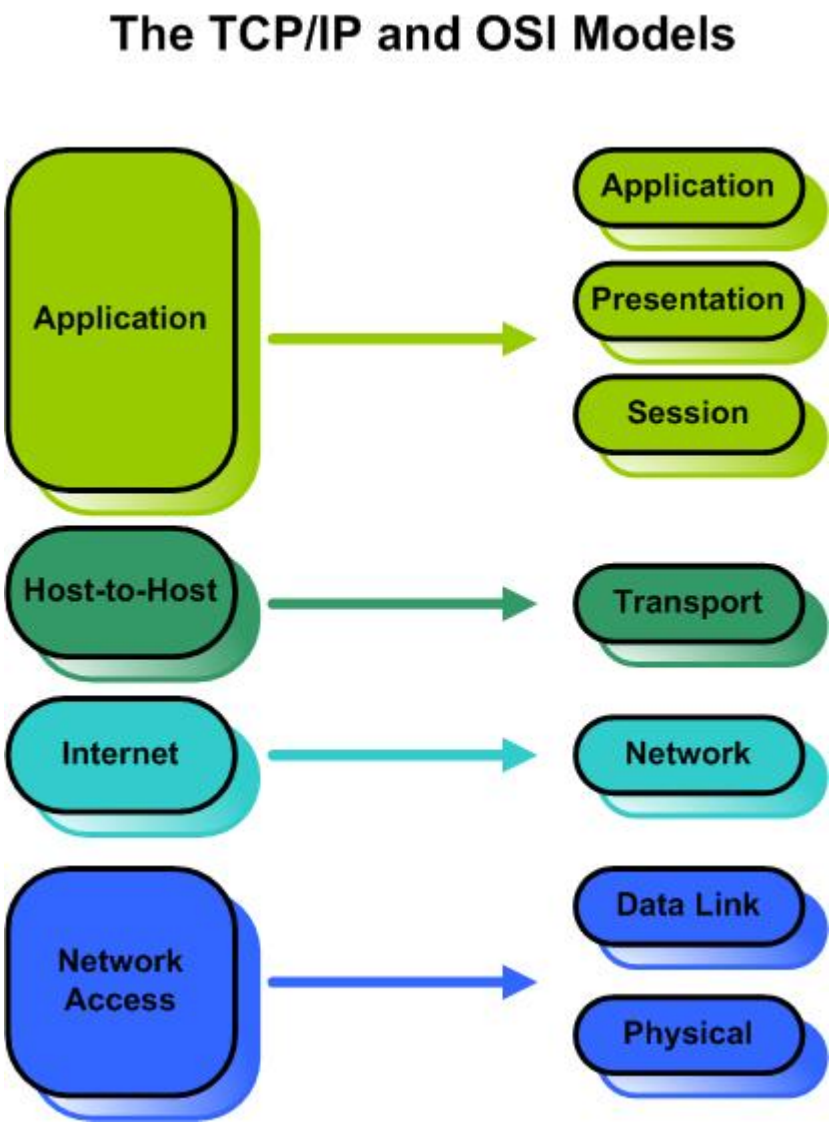
NSRC / IT University of Copenhagen

Last edit: February 2012, ICTP Trieste

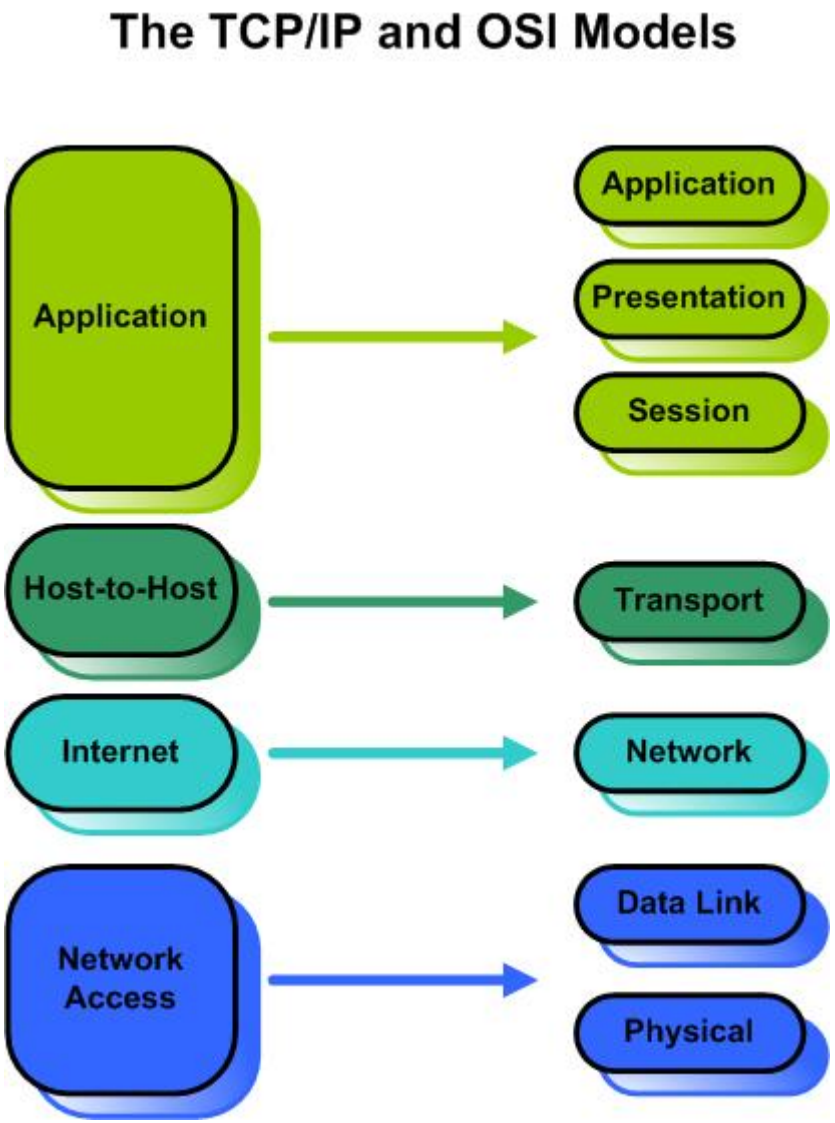
Agenda

- What is network monitoring?
- The ”big three”
- Other useful tools and systems
- Questions and discussion

Remember the layer model



Remember the layer model



- General Network monitoring

  mostly works on layer 3 and up, and often assumes TCP/IP networks

- Wireless network monitoring

  typically involves layer 2 - the specifically wireless aspects (spectrum, SSIDs, etc)

What are we monitoring?

- Connections, links, quality
- bandwidth, usage
- performance
- systems & services
- resources
- configurations, changes
- logfiles
- users?
- content of traffic?

Monitoring & Management

- Monitoring without response does not make much sense -

  what good is seeing a problem if you dont react?

- Monitoring is part of management

- Management is closely related to

  expectations, contracts, SLAs

Different types of monitoring

- **human operated** vs **automatic**
- **active** vs **passive**
- Active human operated monitoring often gives good insight, but is not feasible 24/7
- Automatic monitoring can run 24/7, but needs to trigger notification/alerts and file service tickets in order to be useful
- Often the combination of both is needed.

The “big three”

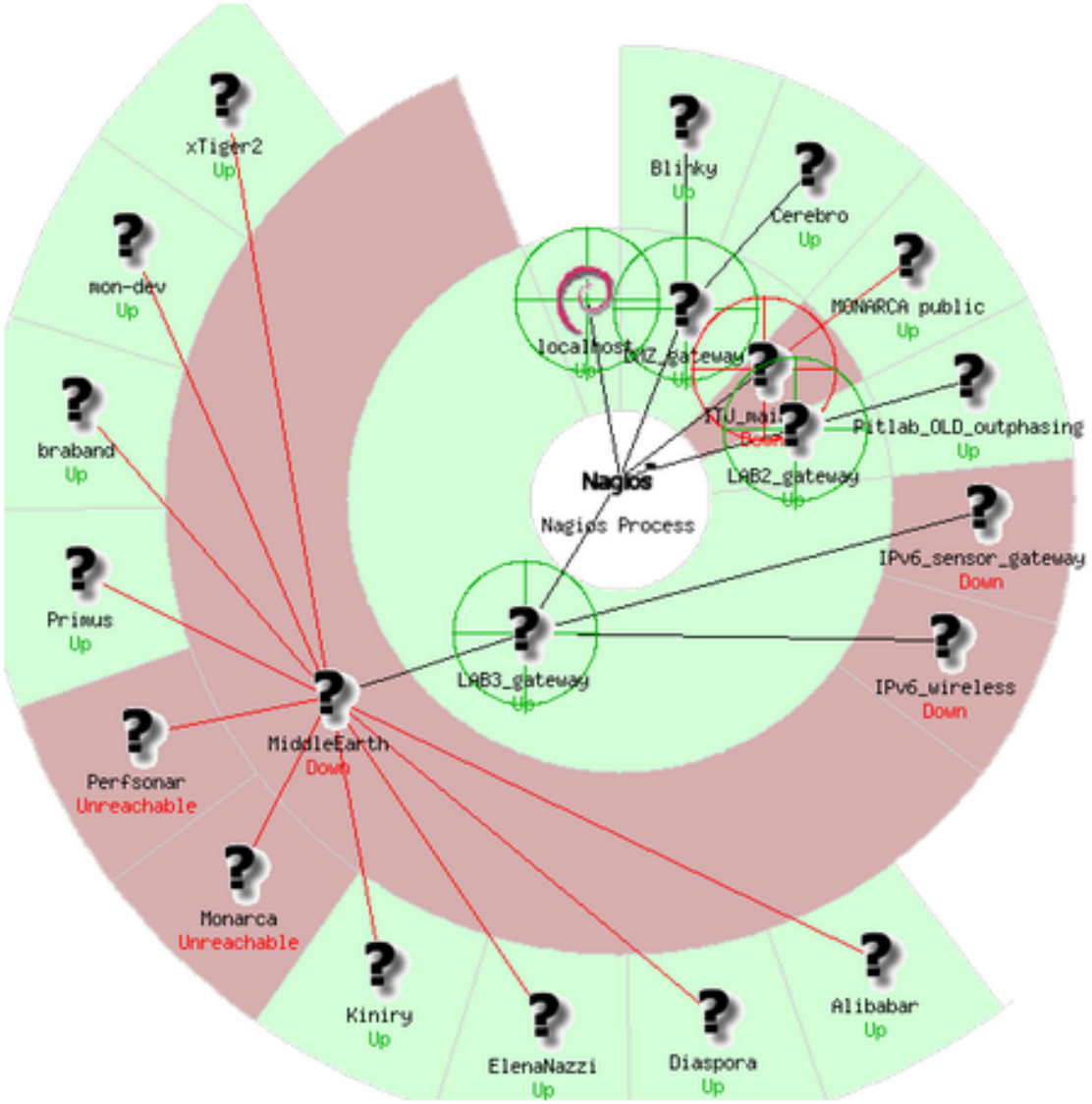
- **Nagios**
  servers, switches, devices, services & anything that can talk IP and/or SNMP (this can include small wireless sensors!)
- **Smokeping**
  connections, quality, ping rtt, latency, jitter
- **Cacti**
  resources, traffic, interfaces, transactions, .. almost anything that is accessible via SNMP, e.g. temperature, power, ... sensor data

Nagios

- Nagios is an open source computer system monitor, network monitoring and infrastructure monitoring software application.
  Nagios offers monitoring and alerting for servers, switches, applications, and services. It watches hosts and services, alerting users when things go wrong and again when they get better.

  (source: wikipedia)

Nagios


xTiger2
Up
Blinky
Up
Cerebro
Up
mon-dev
Up
MONARCA public
Up
localhost
Up
LOZ_gateway
Up
braband
Up
KTU_mail
Down
Pitlab_OLD_outphasing
Up
LAB2_gateway
Up
Nagios
Nagios Process
IPv6_sensor_gateway
Down
Primus
Up
LAB3_gateway
Up
IPv6_wireless
Down
MiddleEarth
Down
Perfsonar
Unreachable
Monarca
Unreachable
Kiniry
Up
ElenaNazzi
Up
Diaspora
Up
Alibabar
Up

Nagios

Current Network Status
Last Updated: Tue Feb 14 22:50:05 CET 2012
Updated every 90 seconds
Nagios® Core™ 3.2.0 - www.nagios.org
Logged in as *nagiosadmin*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
16	4	2	0

All Problems	All Types
6	22

Se

Ok	Warning
13	0

All

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
Alibabar	UP	2012-02-14 22:47:41	355d 10h 34m 29s	PING OK - Packet loss = 0%, RTA = 0.25 ms
Blinky	UP	2012-02-14 22:49:01	69d 8h 22m 14s	PING OK - Packet loss = 0%, RTA = 0.93 ms
Cerebro	UP	2012-02-14 22:49:11	69d 8h 22m 4s	PING OK - Packet loss = 0%, RTA = 0.57 ms
DMZ_gateway	UP	2012-02-14 22:49:31	69d 8h 22m 4s	PING OK - Packet loss = 0%, RTA = 1.43 ms
Diaspora	UP	2012-02-14 22:48:31	144d 10h 55m 59s	PING OK - Packet loss = 0%, RTA = 0.22 ms
ElenaNazzi	UP	2012-02-14 22:49:51	71d 6h 41m 4s	PING OK - Packet loss = 0%, RTA = 0.29 ms
IPv6_sensor_gateway	DOWN	2012-02-14 22:49:11	1d 14h 4m 24s	CRITICAL - Host Unreachable (130.226.142.166)
IPv6_wireless	DOWN	2012-02-14 22:49:41	1d 14h 3m 54s	CRITICAL - Host Unreachable (130.226.142.169)
ITU_main_fw	DOWN	2012-02-14 22:47:41	237d 12h 51m 39s	CRITICAL - Host Unreachable (130.226.142.142)
Kinny	UP	2012-02-14 22:49:31	78d 12h 37m 54s	PING OK - Packet loss = 0%, RTA = 0.58 ms
LAB2_gateway	UP	2012-02-14 22:49:51	140d 7h 41m 0s	PING OK - Packet loss = 0%, RTA = 1.42 ms
LAB3_gateway	UP	2012-02-14 22:49:01	35d 13h 53m 54s	PING OK - Packet loss = 0%, RTA = 1.48 ms
MONARCA public	UP	2012-02-14 22:48:41	35d 13h 53m 54s	PING OK - Packet loss = 0%, RTA = 2.30 ms
MiddleEarth	DOWN	2012-02-14 22:45:31	35d 13h 53m 44s	PING CRITICAL - Packet loss = 100%
Monarca	UNREACHABLE	2012-02-14 22:46:41	1d 14h 6m 54s	CRITICAL - Host Unreachable (130.226.142.167)
Perfsonar	UNREACHABLE	2012-02-14 22:45:51	362d 8h 40m 1s	CRITICAL - Host Unreachable (130.226.142.168)
Pitlab_OLD_outphasing	UP	2012-02-14 22:46:51	1d 14h 22m 14s	PING OK - Packet loss = 0%, RTA = 0.25 ms
Primus	UP	2012-02-14 22:46:21	355d 10h 32m 21s	PING OK - Packet loss = 0%, RTA = 0.03 ms
trabant	UP	2012-02-14 22:46:31	78d 12h 40m 4s+	PING OK - Packet loss = 0%, RTA = 2.68 ms
localhost	UP	2012-02-14 22:46:41	564d 9h 30m 57s	PING OK - Packet loss = 0%, RTA = 0.02 ms
man-dev	UP	2012-02-14 22:48:11	33d 19h 32m 24s	PING OK - Packet loss = 0%, RTA = 0.24 ms
xTiger2	UP	2012-02-14 22:47:11	140d 0h 53m 30s	PING OK - Packet loss = 0%, RTA = 3.11 ms

Nagios – how to get started?

- For example by using the NSRC exercises:

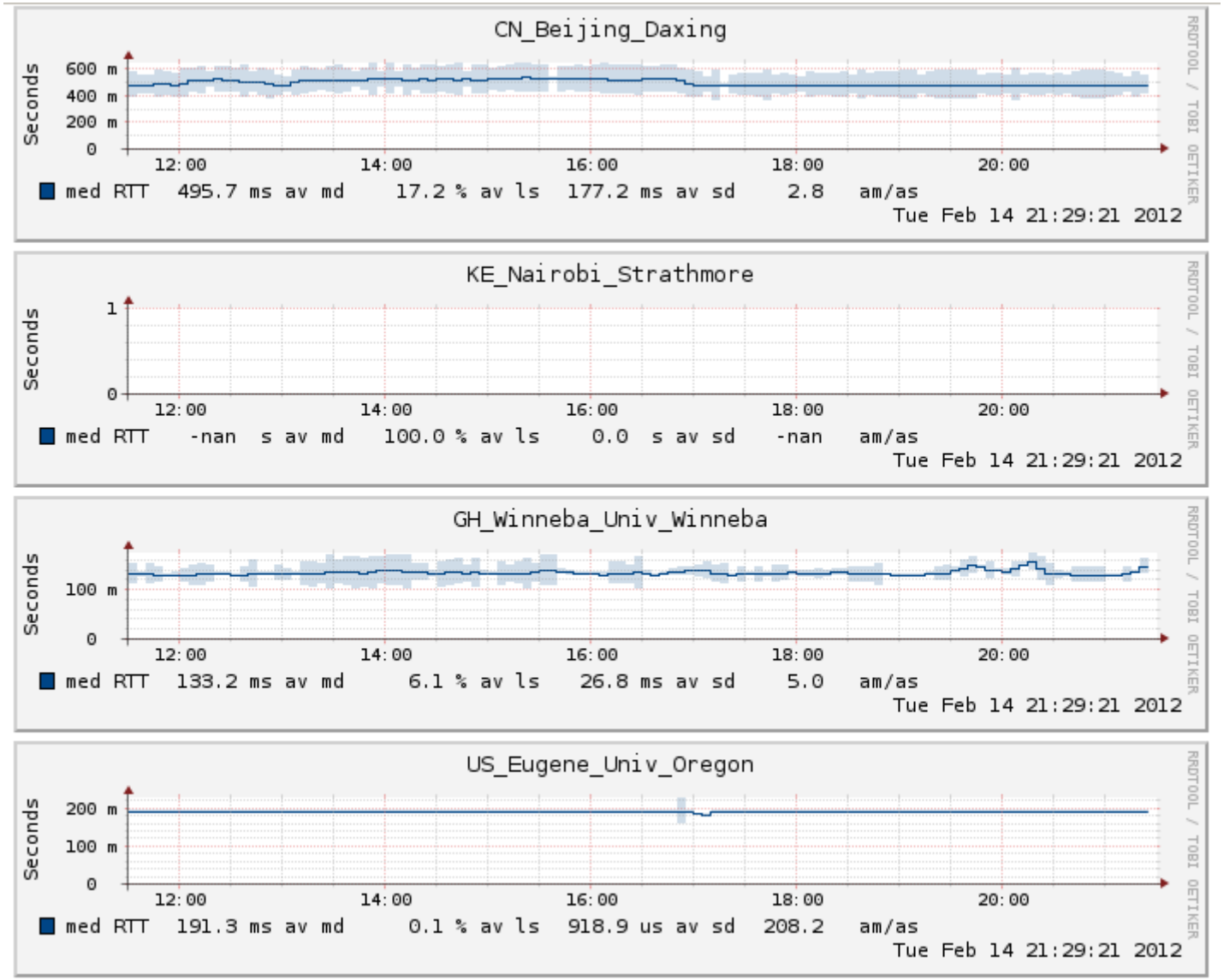
  https://nsrc.org/workshops/ws-files/2011/sanog17/exercises/exercises-nagios.html

  http://nagios.org

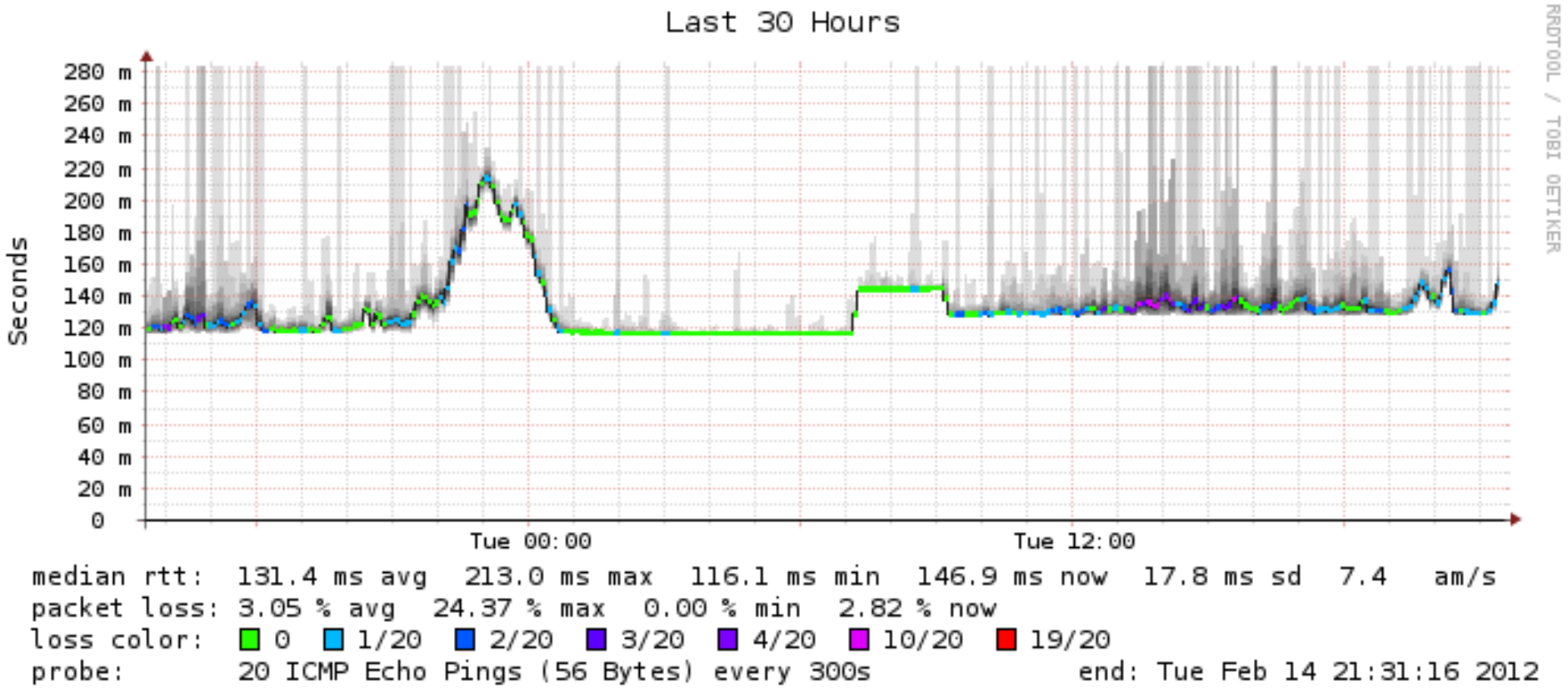
Smokeping

- Smokeping is a network latency monitor. It measures network latency – rtt, jitter - to a configurable set of destinations on the network, and displays its findings in easy-to-read Web pages.
  SmokePing uses RRDtool as its logging and graphing back-end, making the system very efficient. The presentation of the data on the Web is done through a CGI with some AJAX capabilities for interactive graph exploration.
  (source: freshmeat)

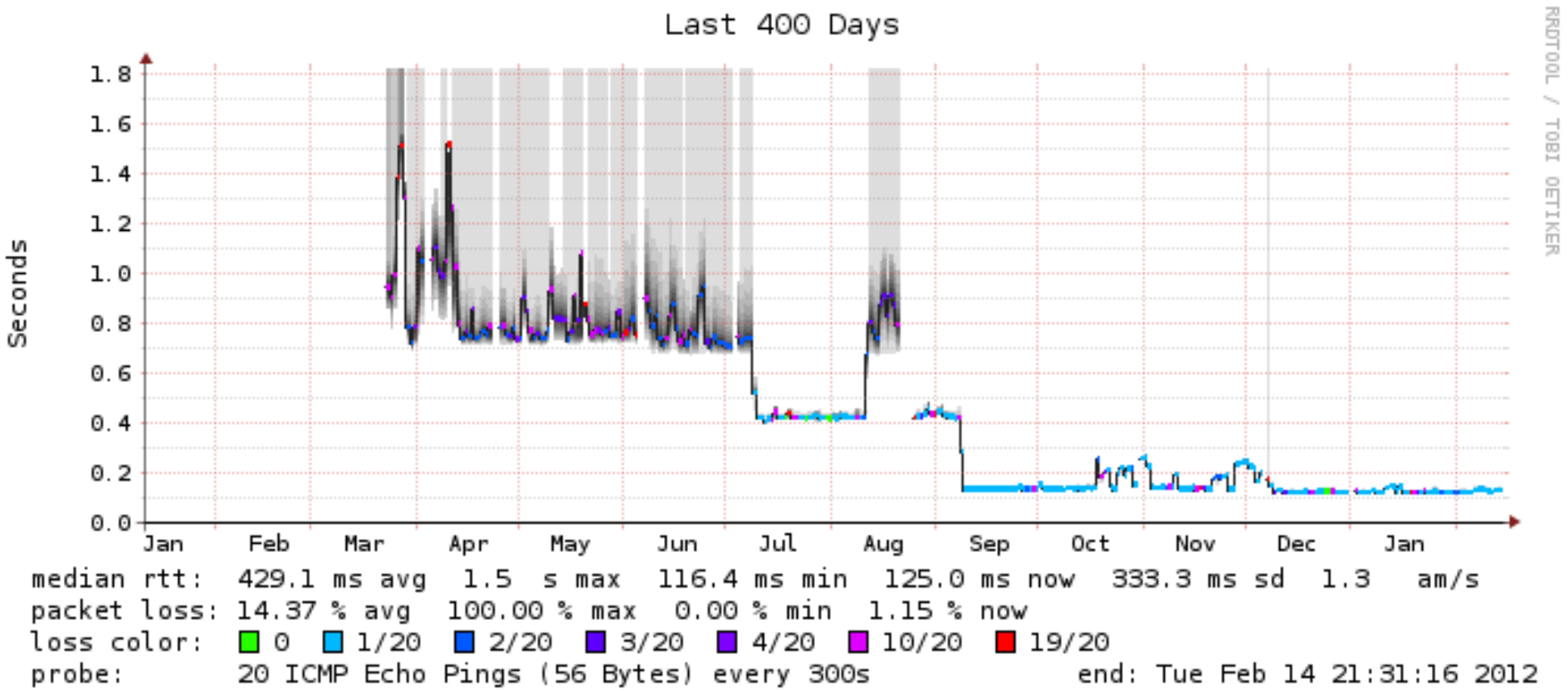
Smokeping


CN_Beijing_Daxing
Seconds
600 m
400 m
200 m
0
12:00
14:00
16:00
18:00
20:00
med RTT 495.7 ms av md 17.2 % av ls 177.2 ms av sd 2.8 am/as
Tue Feb 14 21:29:21 2012
RRDTOOL / TOBI OETIKER
KE_Nairobi_Strathmore
Seconds
1
0
12:00
14:00
16:00
18:00
20:00
med RTT -nan s av md 100.0 % av ls 0.0 s av sd -nan am/as
Tue Feb 14 21:29:21 2012
RRDTOOL / TOBI OETIKER
GH_Winneba_Univ_Winneba
Seconds
100 m
0
12:00
14:00
16:00
18:00
20:00
med RTT 133.2 ms av md 6.1 % av ls 26.8 ms av sd 5.0 am/as
Tue Feb 14 21:29:21 2012
RRDTOOL / TOBI OETIKER
US_Eugene_Univ_Oregon
Seconds
200 m
100 m
0
12:00
14:00
16:00
18:00
20:00
med RTT 191.3 ms av md 0.1 % av ls 918.9 us av sd 208.2 am/as
Tue Feb 14 21:29:21 2012
RRDTOOL / TOBI OETIKER

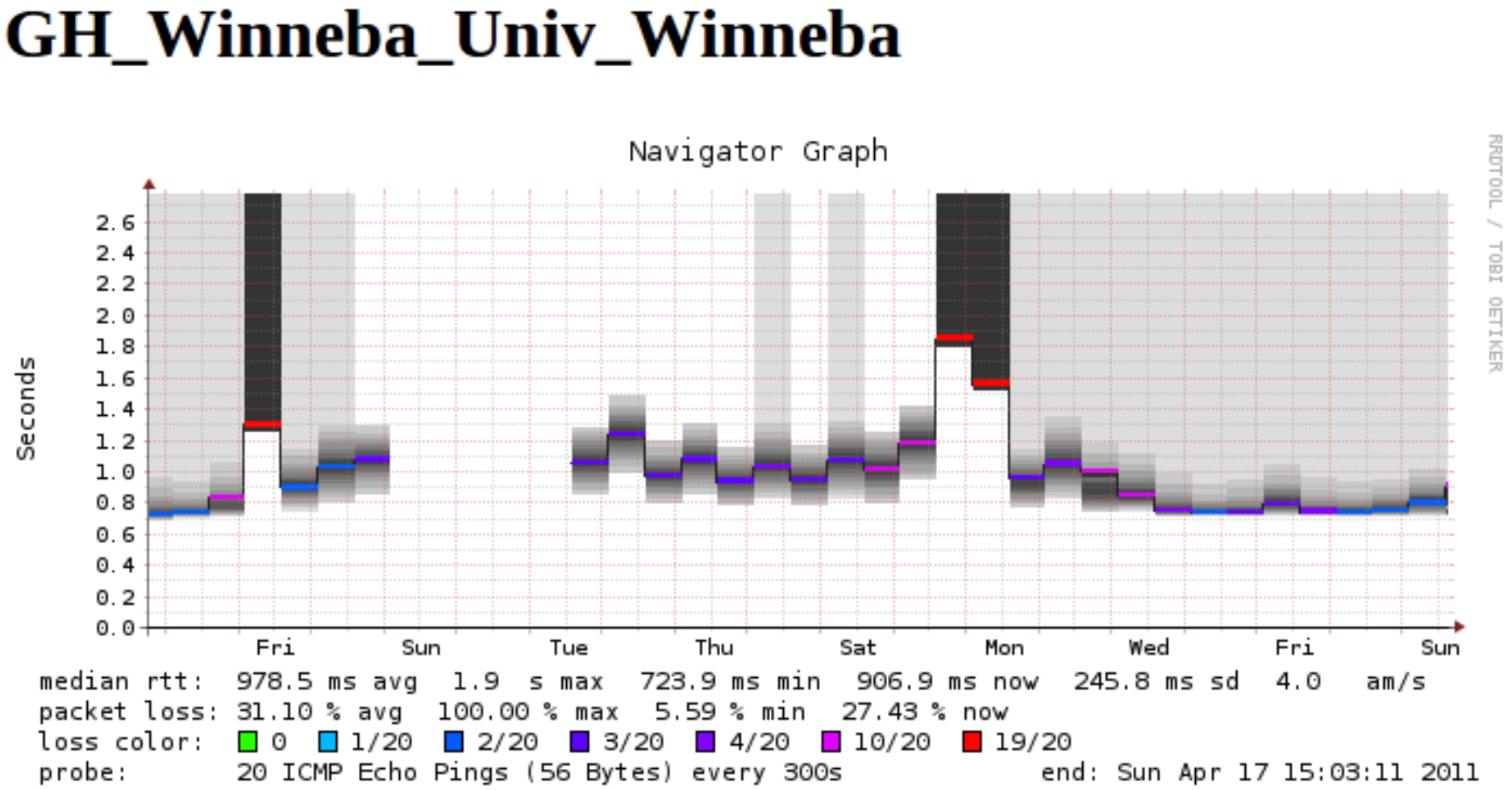
Smokeping


Last 30 Hours
Seconds
280 m
260 m
240 m
220 m
200 m
180 m
160 m
140 m
120 m
100 m
80 m
60 m
40 m
20 m
0
Tue 00:00
Tue 12:00
RRDTOOL / TOBI OETIKER
median rtt: 131.4 ms avg 213.0 ms max 116.1 ms min 146.9 ms now 17.8 ms sd 7.4 am/s
packet loss: 3.05 % avg 24.37 % max 0.00 % min 2.82 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s
end: Tue Feb 14 21:31:16 2012

Smokeping

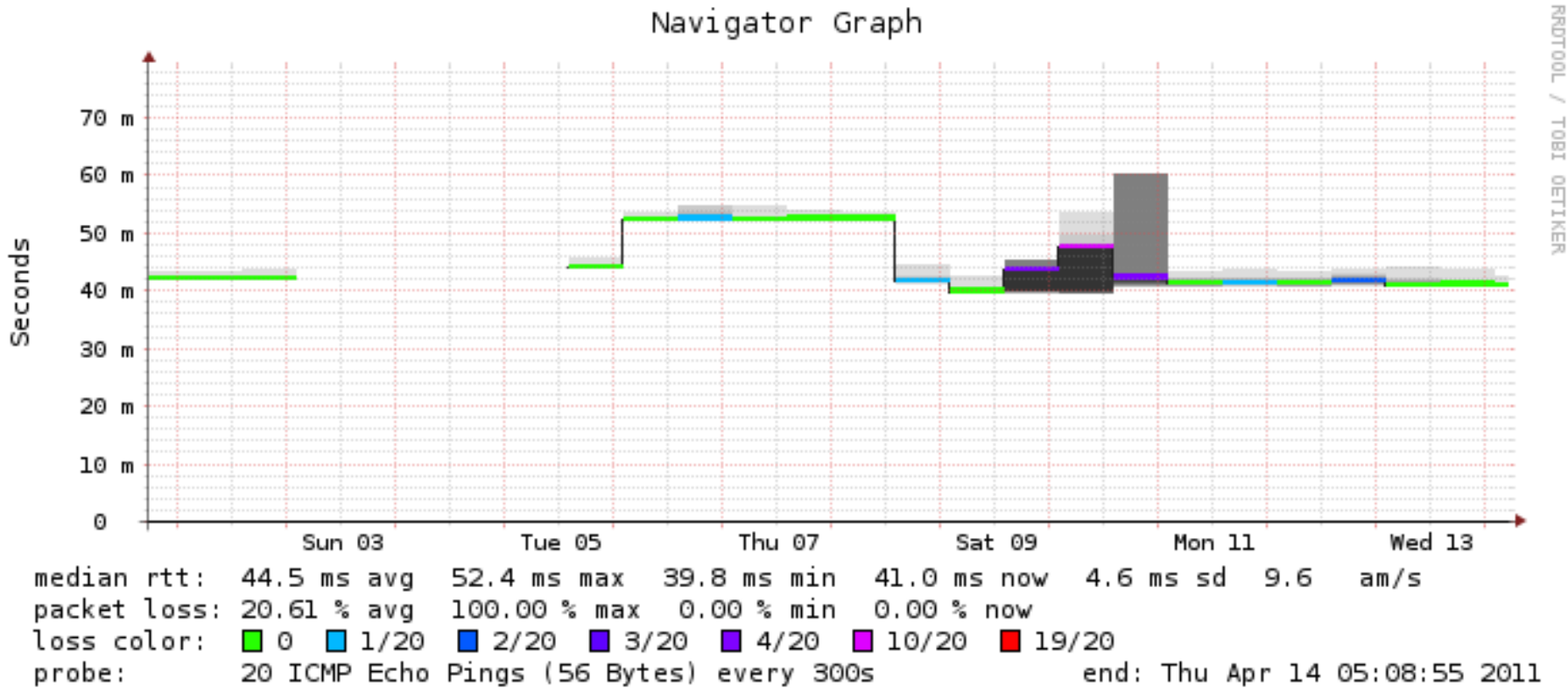

Last 400 Days
Seconds
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
RRDTOOL / TOBI OETIKER
median rtt: 429.1 ms avg 1.5 s max 116.4 ms min 125.0 ms now 333.3 ms sd 1.3 am/s
packet loss: 14.37 % avg 100.00 % max 0.00 % min 1.15 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s
end: Tue Feb 14 21:31:16 2012

Smokeping


GH_Winneba_Univ_Winneba
Navigator Graph
Seconds
2.6
2.4
2.2
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Fri
Sun
Tue
Thu
Sat
Mon
Wed
Fri
Sun
median rtt: 978.5 ms avg 1.9 s max 723.9 ms min 906.9 ms now 245.8 ms sd 4.0 am/s
packet loss: 31.10 % avg 100.00 % max 5.59 % min 27.43 % now
loss color: 0 1/20 2/20 3/20 4/20 10/20 19/20
probe: 20 ICMP Echo Pings (56 Bytes) every 300s
end: Sun Apr 17 15:03:11 2011
RRDTOOL / TOBI OETIKER

Smokeping

IT_Trieste_ICTP



Smokeping – how to get started?

- For example by using the NSRC exercises:

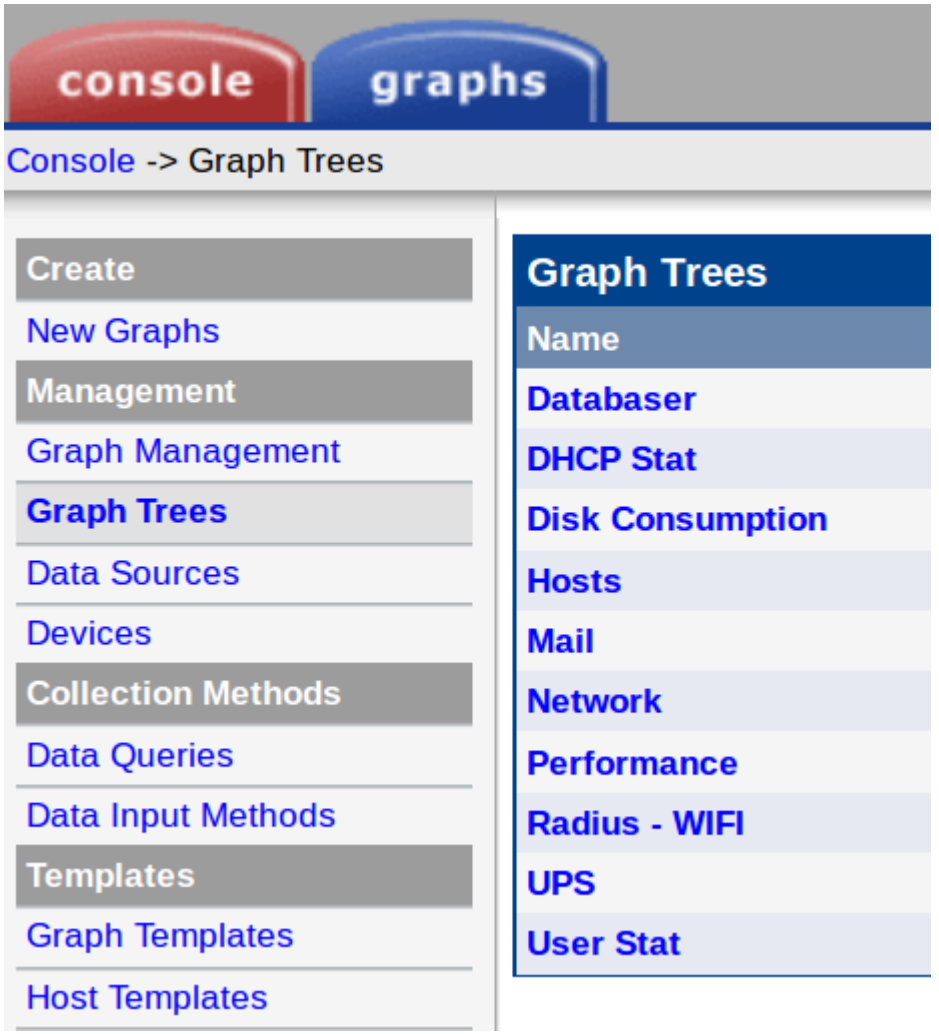
  https://nsrc.org/workshops/ws-files/2011/sanog17/exercises/exercises-smokeping.html

  http://oss.oetiker.ch/smokeping/

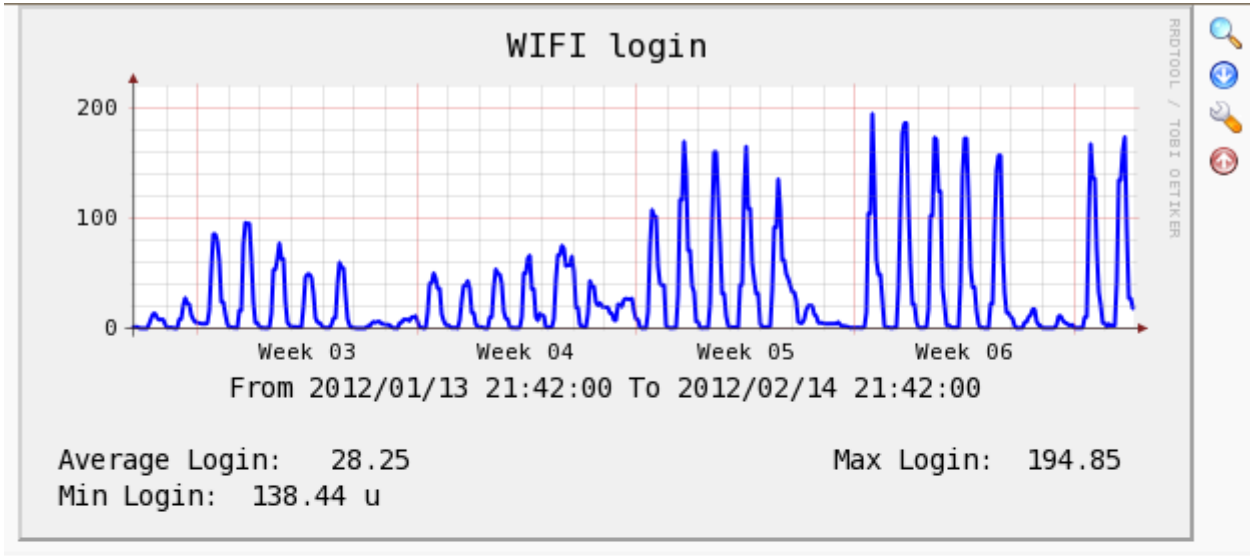
Cacti

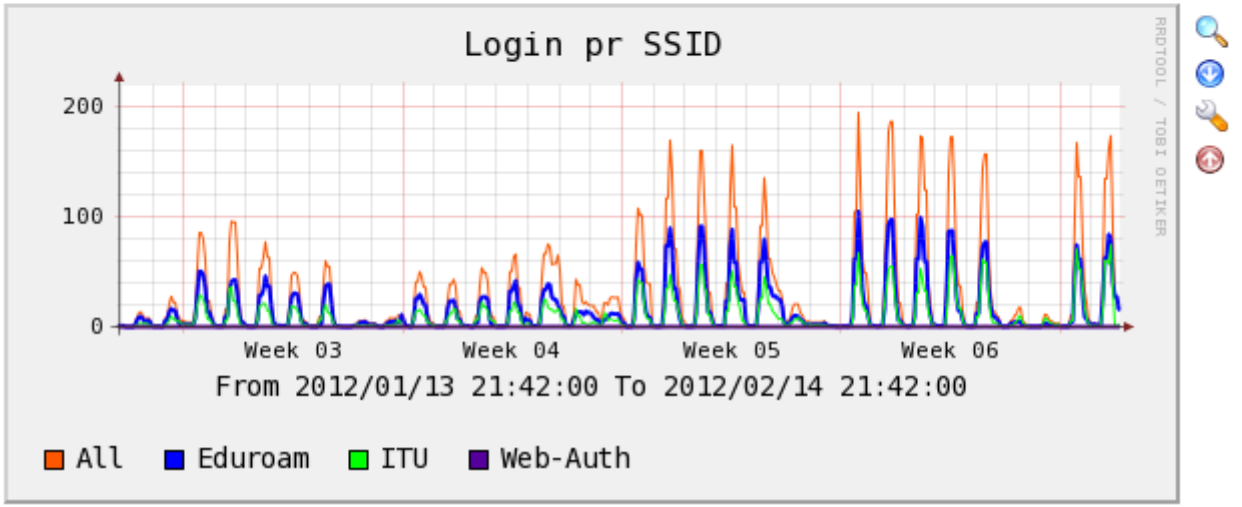
- Cacti is an open source, web-based graphing tool designed as a frontend to RRDtool's data storage and graphing functionality. Cacti allows a user to poll services at predetermined intervals and graph the resulting data. It is generally used to graph time-series data of metrics such as CPU load and network bandwidth utilization. A common usage is to monitor network traffic by polling a network switch or router interface via SNMP.
(source: wikipedia)

Cacti

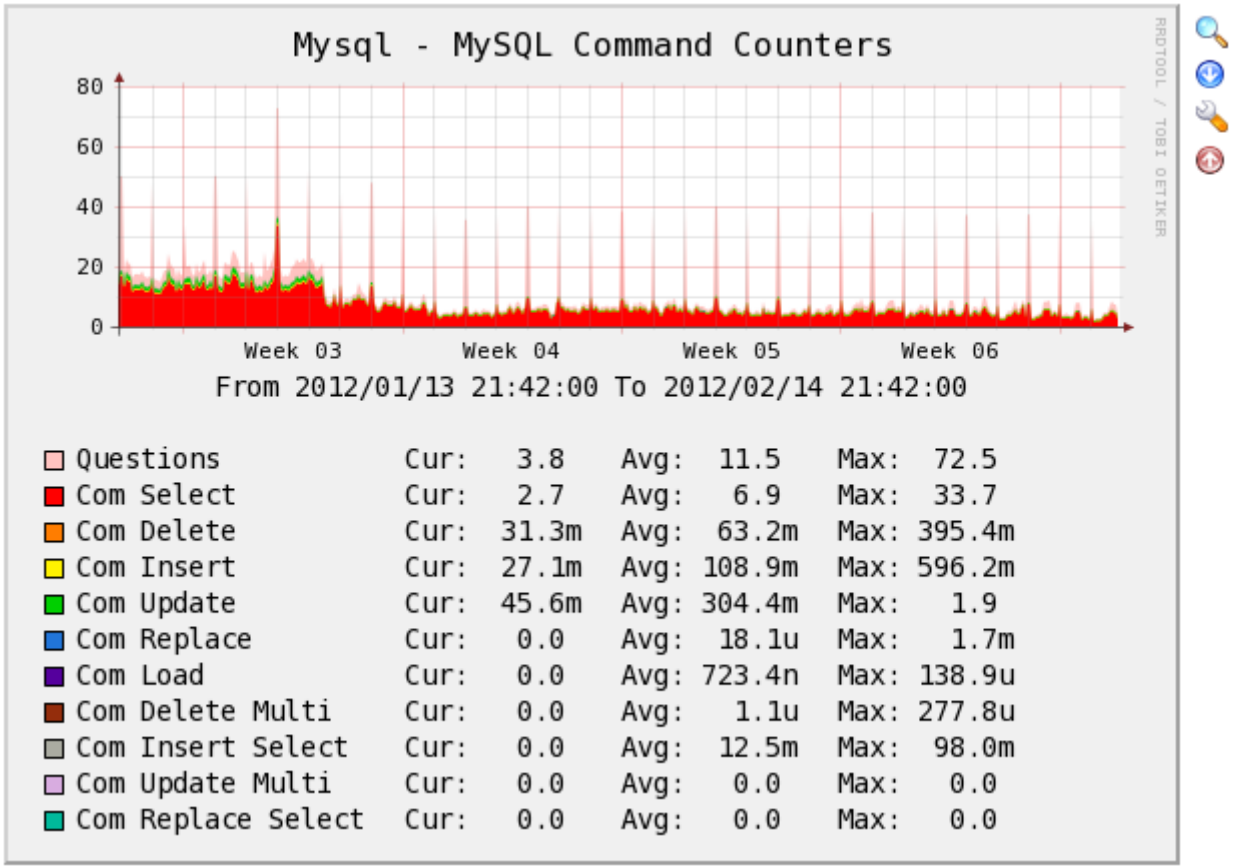

console
graphs
Console -> Graph Trees
Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Graph Trees
Name
Databaser
DHCP Stat
Disk Consumption
Hosts
Mail
Network
Performance
Radius - WIFI
UPS
User Stat

Cacti

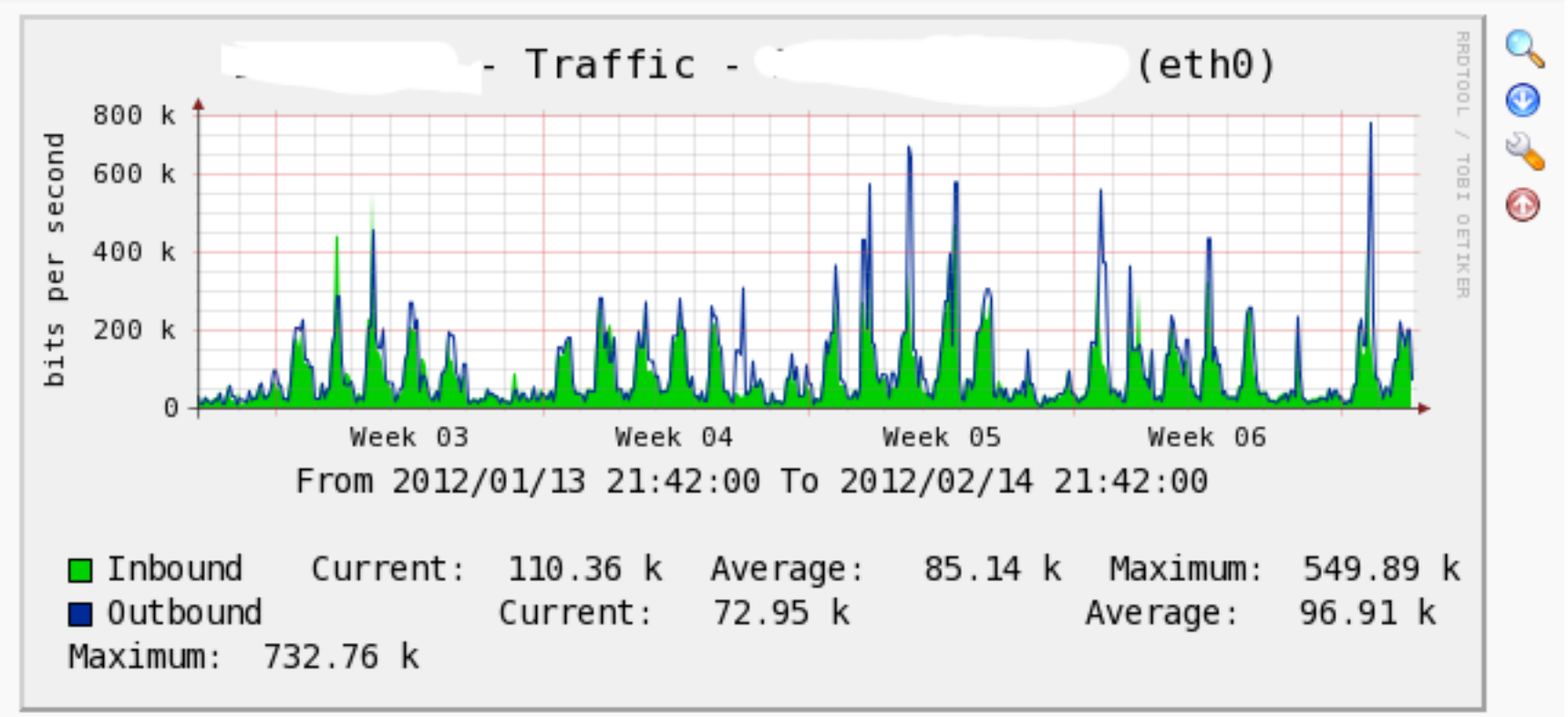

WIFI login
200
100
0
Week 03
Week 04
Week 05
Week 06
From 2012/01/13 21:42:00 To 2012/02/14 21:42:00
Average Login: 28.25
Max Login: 194.85
Min Login: 138.44 u
RRDTOOL / TOBI OETIKER


Login pr SSID
200
100
0
Week 03
Week 04
Week 05
Week 06
From 2012/01/13 21:42:00 To 2012/02/14 21:42:00
All
Eduroam
ITU
Web-Auth
RRDTOOL / TOBI OETIKER

Cacti


Mysql - MySQL Command Counters
80
60
40
20
0
Week 03
Week 04
Week 05
Week 06
From 2012/01/13 21:42:00 To 2012/02/14 21:42:00
Questions Cur: 3.8 Avg: 11.5 Max: 72.5
Com Select Cur: 2.7 Avg: 6.9 Max: 33.7
Com Delete Cur: 31.3m Avg: 63.2m Max: 395.4m
Com Insert Cur: 27.1m Avg: 108.9m Max: 596.2m
Com Update Cur: 45.6m Avg: 304.4m Max: 1.9
Com Replace Cur: 0.0 Avg: 18.1u Max: 1.7m
Com Load Cur: 0.0 Avg: 723.4n Max: 138.9u
Com Delete Multi Cur: 0.0 Avg: 1.1u Max: 277.8u
Com Insert Select Cur: 0.0 Avg: 12.5m Max: 98.0m
Com Update Multi Cur: 0.0 Avg: 0.0 Max: 0.0
Com Replace Select Cur: 0.0 Avg: 0.0 Max: 0.0
RRDTOOL / TOBI OETIKER

Cacti


- Traffic - (eth0)
bits per second
800 k
600 k
400 k
200 k
0
Week 03
Week 04
Week 05
Week 06
From 2012/01/13 21:42:00 To 2012/02/14 21:42:00
Inbound Current: 110.36 k Average: 85.14 k Maximum: 549.89 k
Outbound Current: 72.95 k Average: 96.91 k
Maximum: 732.76 k
RRDTOOL / TOBI OETIKER

Cacti

- Cacti
  is a good tool for monitoring power
- e.g. solar installations

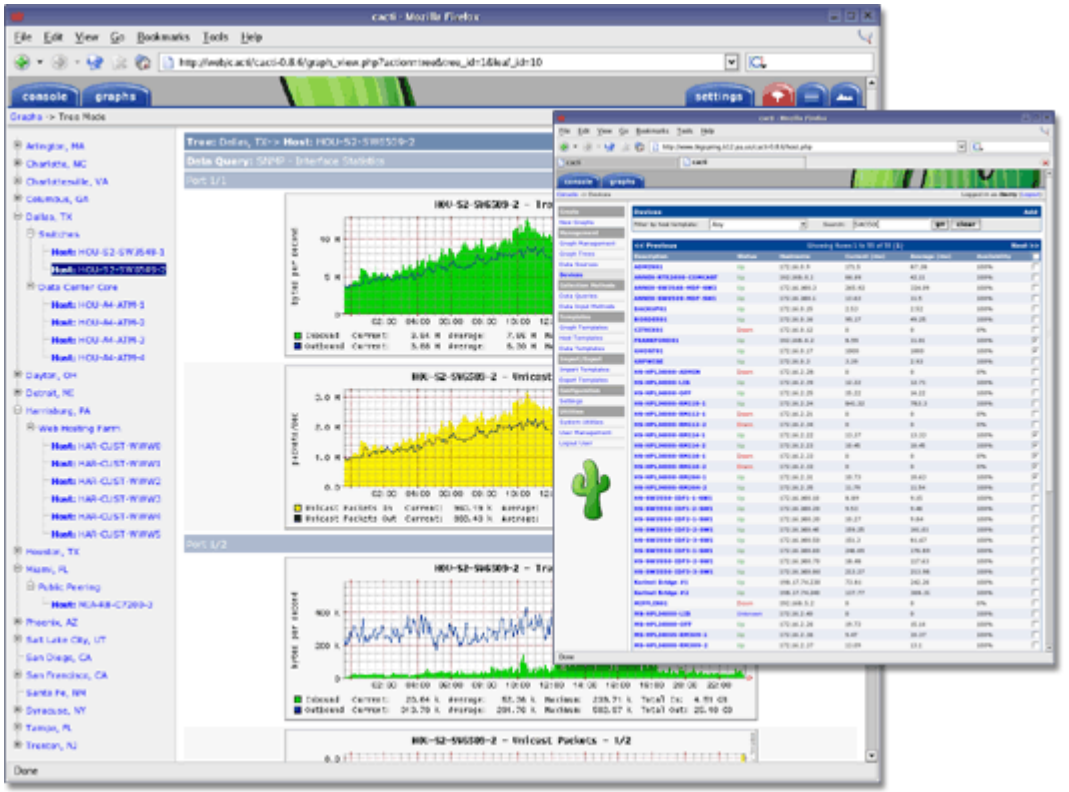
  as it can monitor electrical and environmental data

Cacti – how to get started?

- By now you can guess :)

https://nsrc.org/workshops/2011/afnog-nm/raw-attachment/wiki/Agenda/cacti.pdf

http://cacti.net



SNMP

- **Simple Network Management Protocol (SNMP)** is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more."[1] It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. [2]

- SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications..
(source: wikipedia)

Other useful tools

- Command line tools:

  mtr – ping and traceroute
  nmap – port scanning

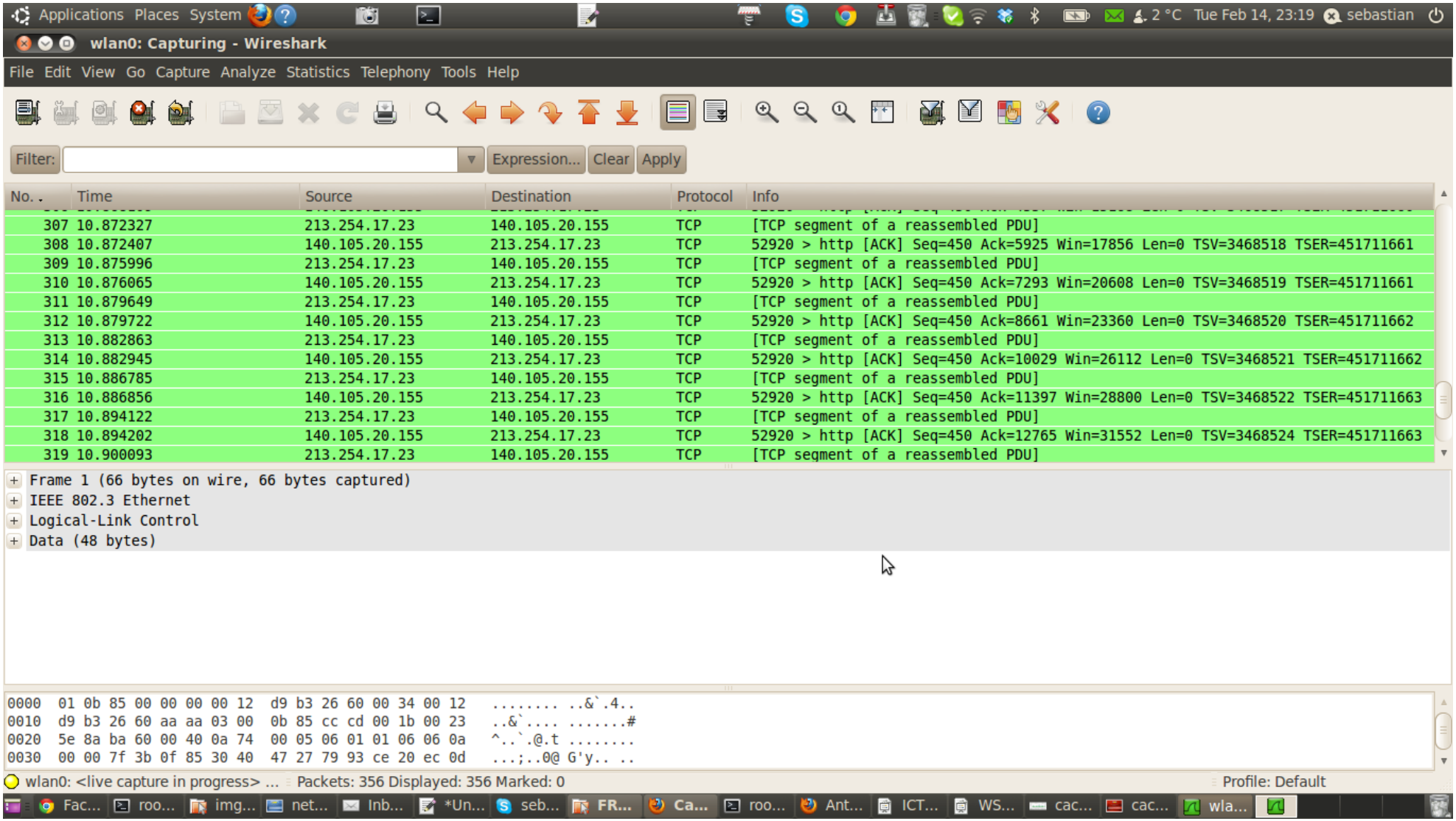
- Iperf
  command line client-server tests

```
# iperf -c 130.226.142.162

Client connecting to 130.226.142.162, TCP port 5001
TCP window size: 16.0 KByte (default)
[  3] local 140.105.20.155 port 50523 connected
with 130.226.142.162 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  24.3 MBytes  20.4 Mbits/sec
```

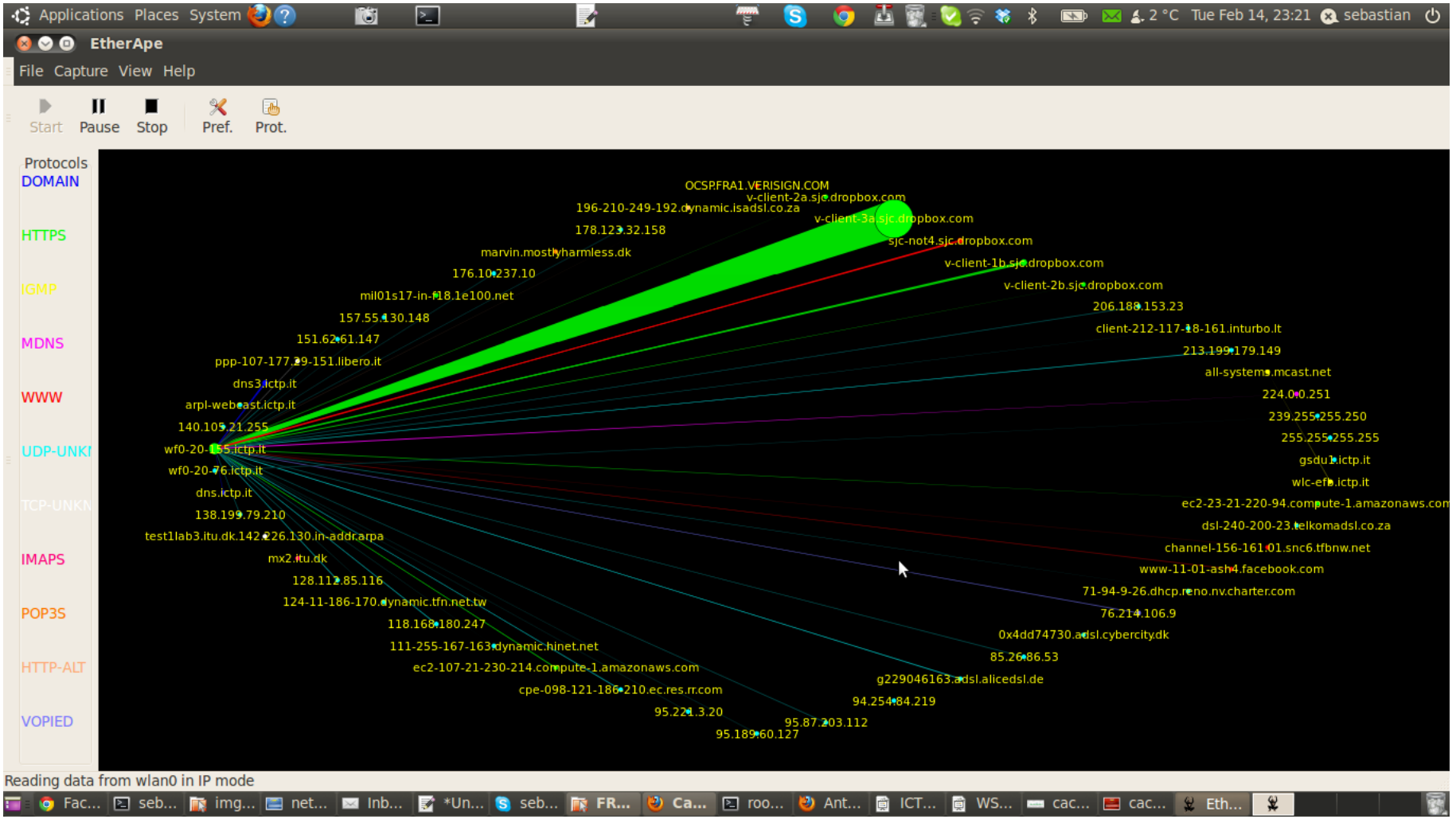
Other useful tools

- Wireshark: advanced packet dumper



Other useful tools

- Etherape: visualization toy, but a nice toy :)



Other useful tools

- Huge performance suite: perfSONAR
- Traffic, bandwidth: bandwidthd
- Router config management: Rancid
- Network Documentation: Netdot
  https://netdot.uoregon.edu/
- Intrusion Detection: tripwire, snort
- Vulnerabilities: Nessus, OpenVAS

And ...

- There are dozens of others ...

  ... but I really have to go to bed now :)

  Questions?

- You tell me what you would like to monitor

  and we find the right tool for it!

Other useful tools

- Huge performance suite: perfSONAR
- Traffic, bandwidth: bandwidthd
- Router config management: Rancid
- Network Documentation: Netdot
  https://netdot.uoregon.edu/
- Intrusion Detection: tripwire, snort
- Vulnerabilities: Nessus, OpenVAS