

Monitoring and Troubleshooting Wireless Campus Networks

Network Startup Resource Center
www.nsrc.org



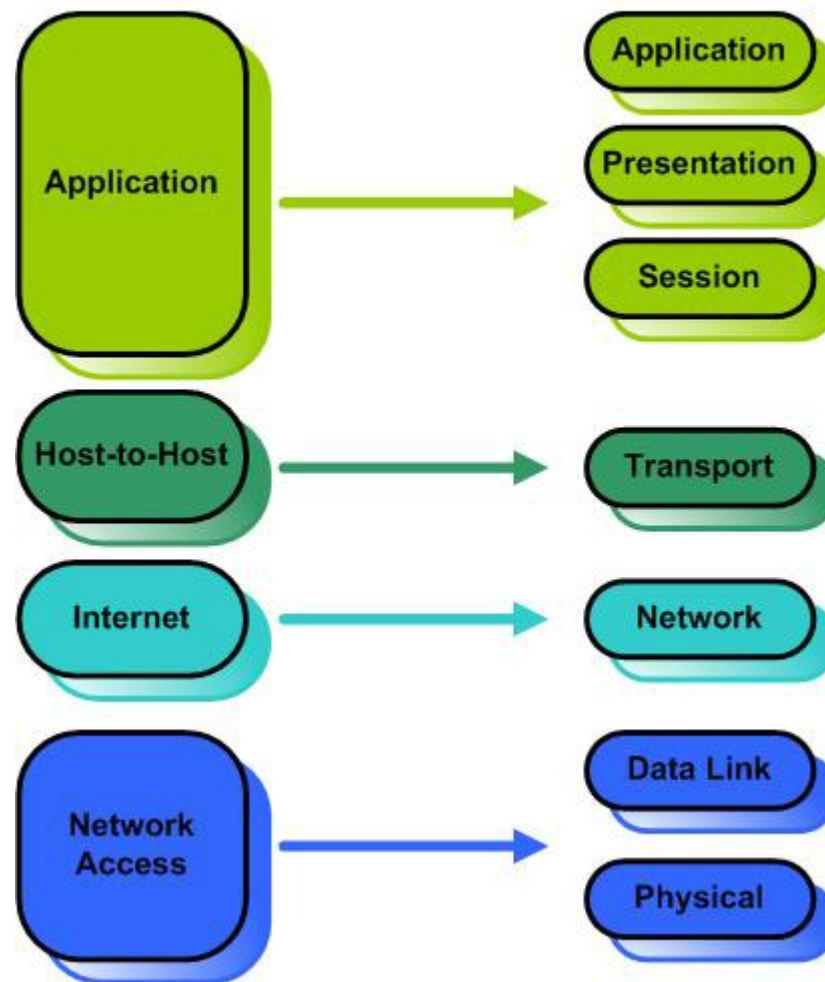
These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(<http://creativecommons.org/licenses/by-nc/4.0/>)

Agenda

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

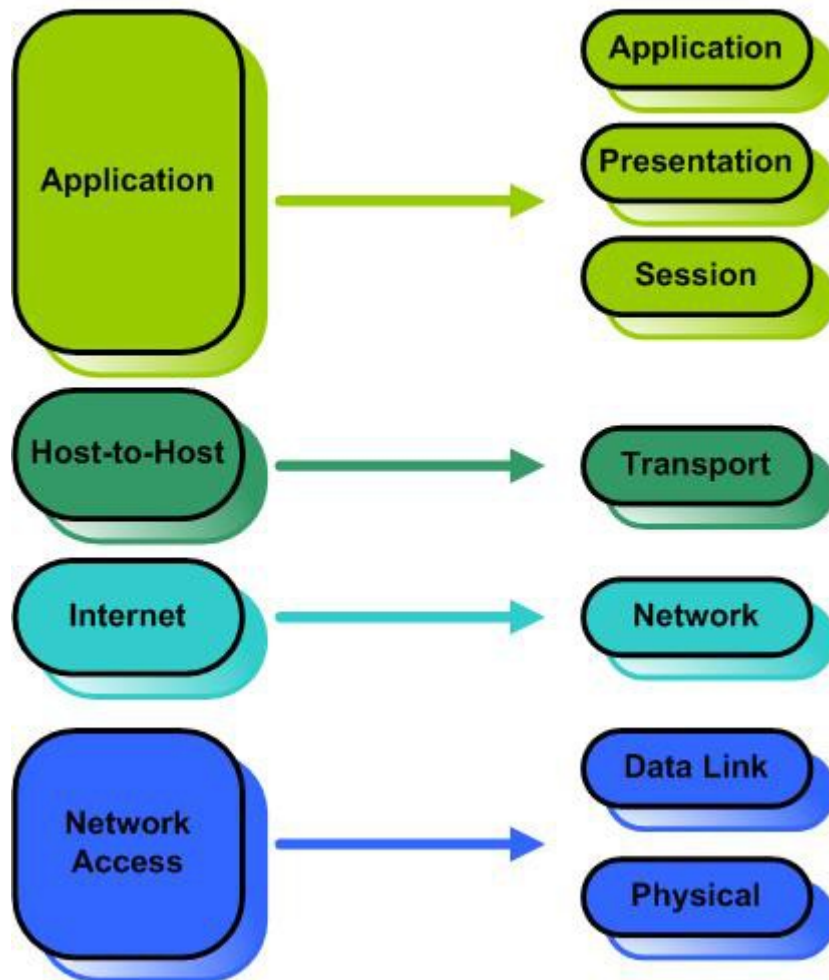
Remember the layer model

The TCP/IP and OSI Models



Remember the layer model

The TCP/IP and OSI Models



- 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 don't 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”

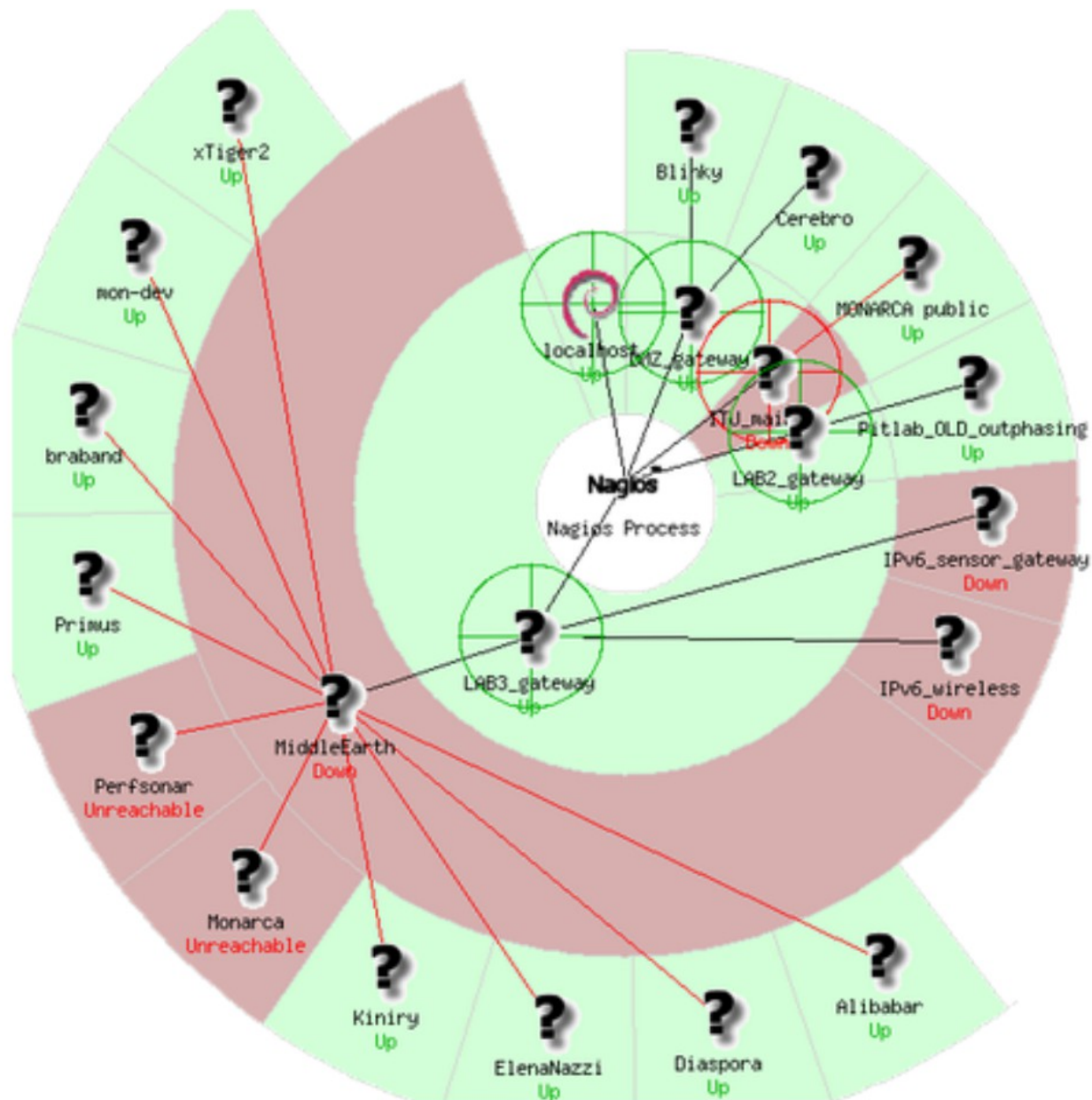
- **Nagios**
servers, switches, devices, services & anything that can talk IP and/or SNMP
(this can include small wireless sensors!)
- **Smokeping**
connections, quality, ping rtt, latency, jitter
- **Cacti**
resources, traffic, interfaces, transactions, .. almost anything that is accessible via SNMP,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



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
10	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
Alibaba	UP	2012-02-14 22:47:41	355d 10h 34m 29s	PING OK - Packet loss = 0%, RTA = 0.25 ms
Binky	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
ElenaHazzi	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 (130.226.142.160)
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)
Kinky	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)
Pertsolar	UNREACHABLE	2012-02-14 22:45:51	362d 8h 40m 1s	CRITICAL - Host Unreachable (130.226.142.168)
Pylab_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
Graband	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
mon-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?

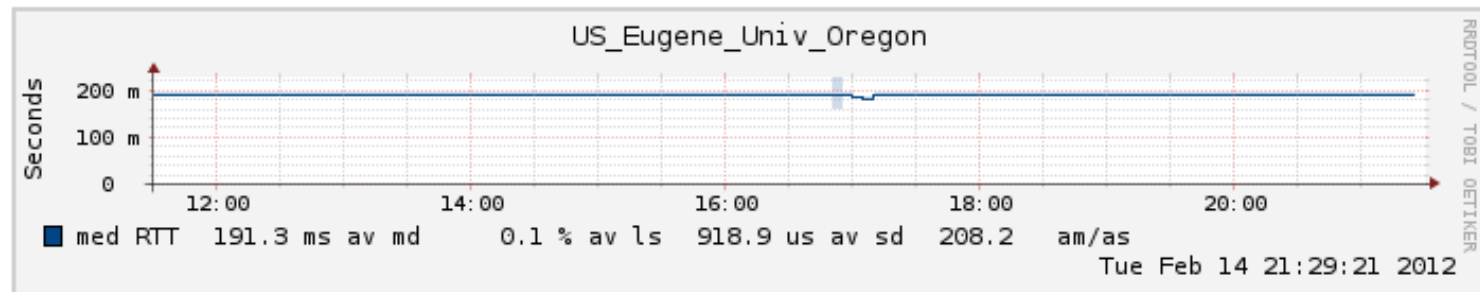
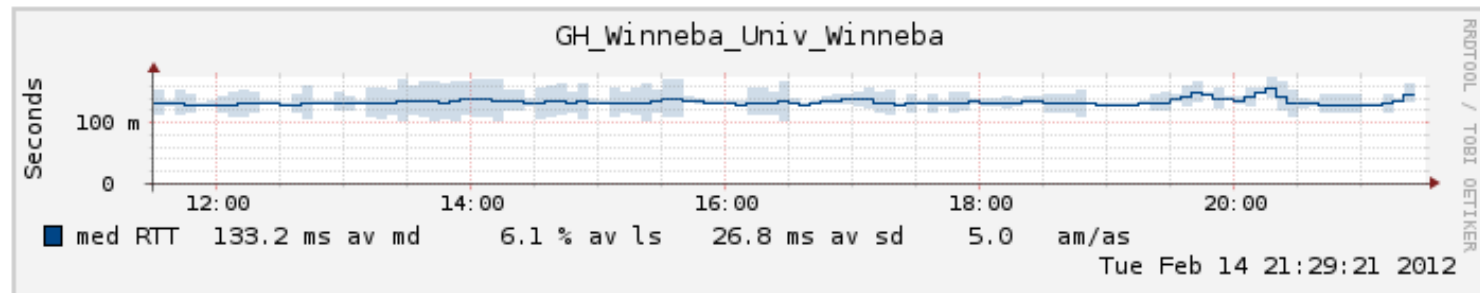
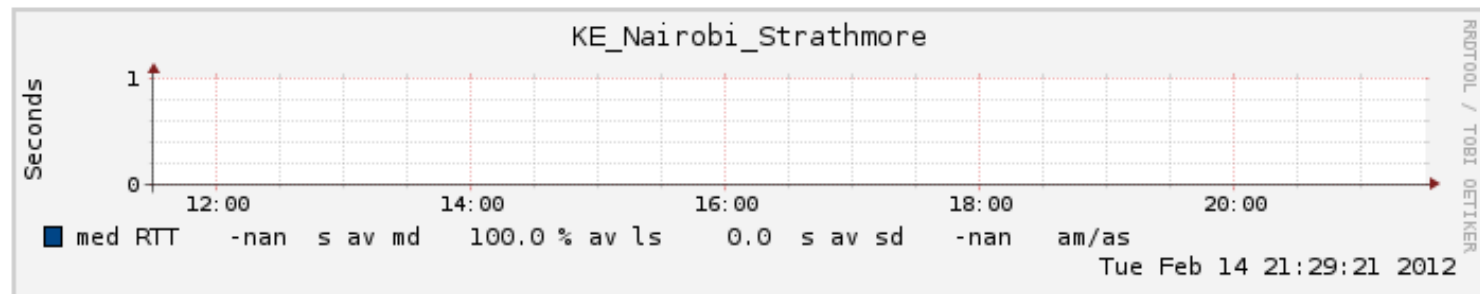
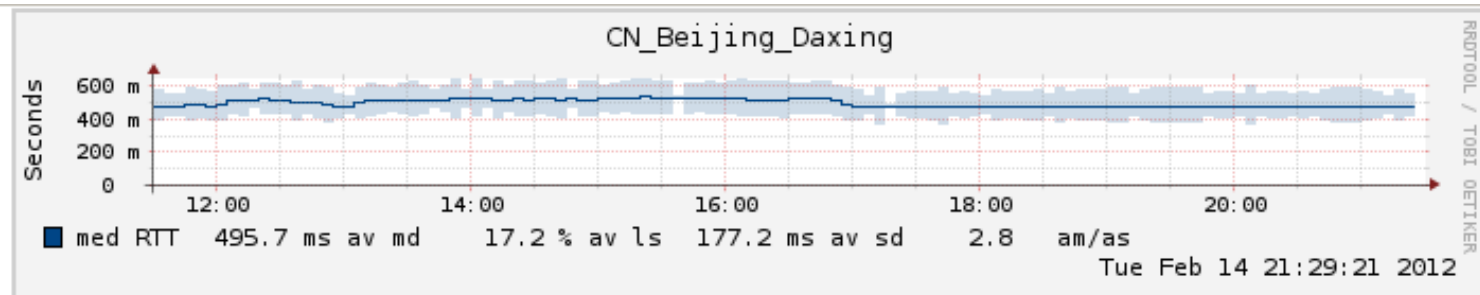
- For example, by using the NSRC exercises:
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/exercises-nagios-I-III-basic.htm>
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/exercises-nagios-IV-VIII-medium.htm>
 - <http://nagios.org>

Smokeping

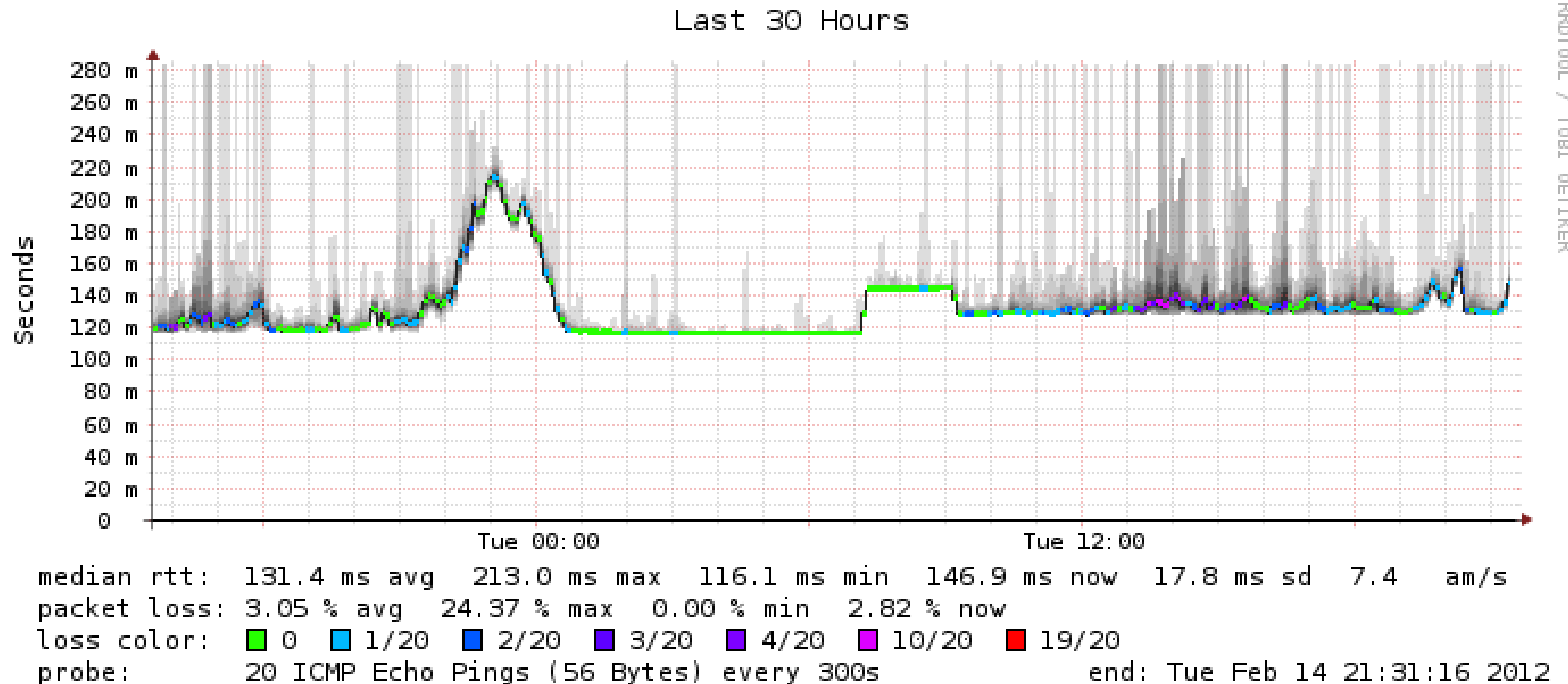
- Smokeping is a network latency monitor. It measures network latency – rtt, jitter - to a configurable set of destinations on the network, and displays its findings in easy-to-read Web pages.
- SmokePing uses RRDtool as its logging and graphing back-end, making the system very efficient. The presentation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

(source: freshmeat)

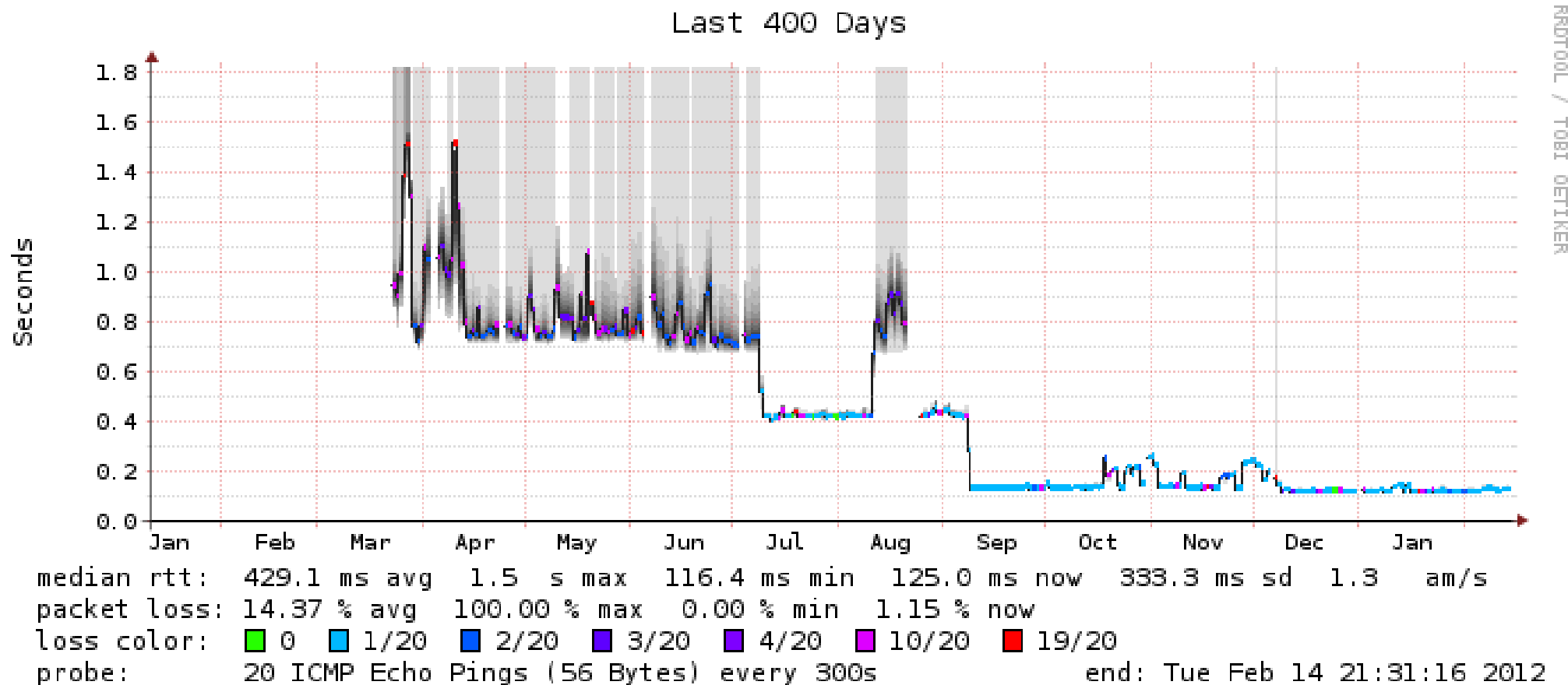
Smokeping



Smokeping

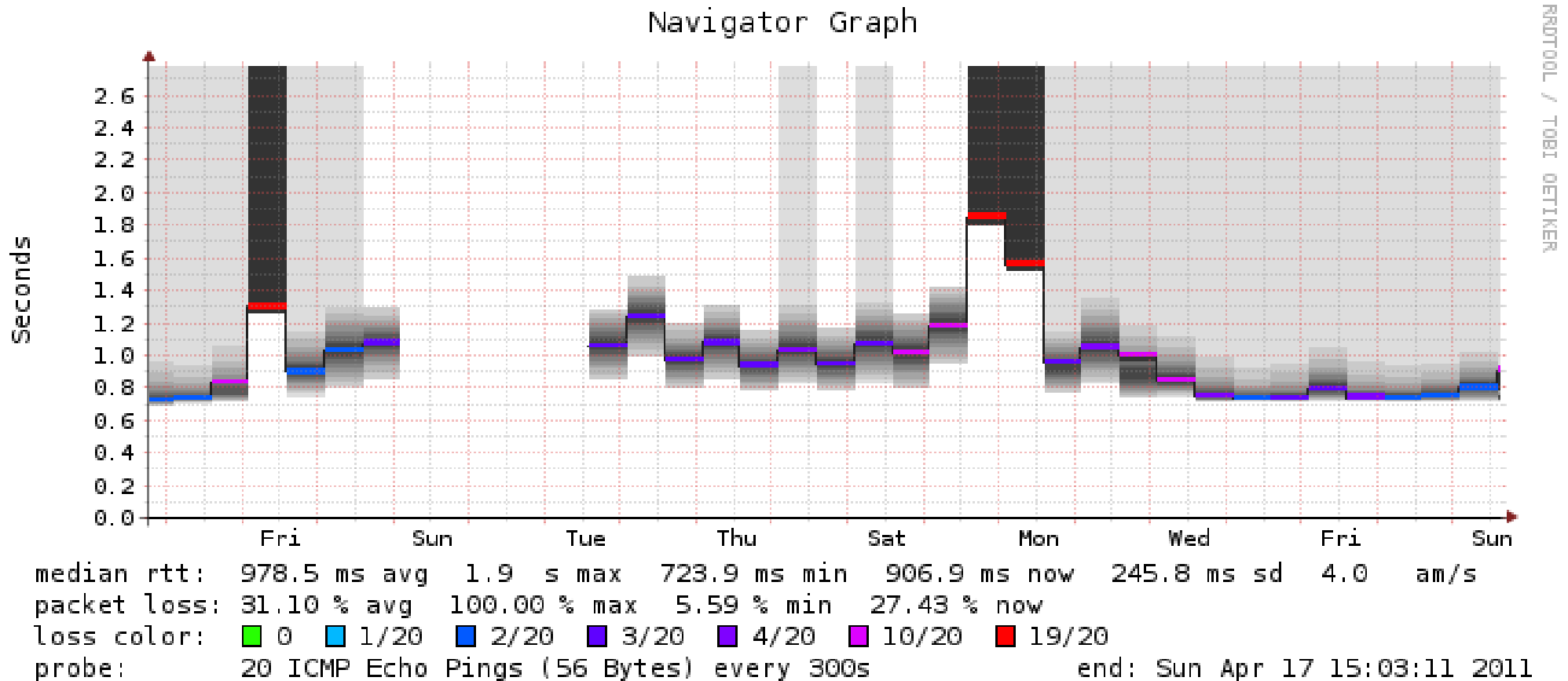


Smokeping



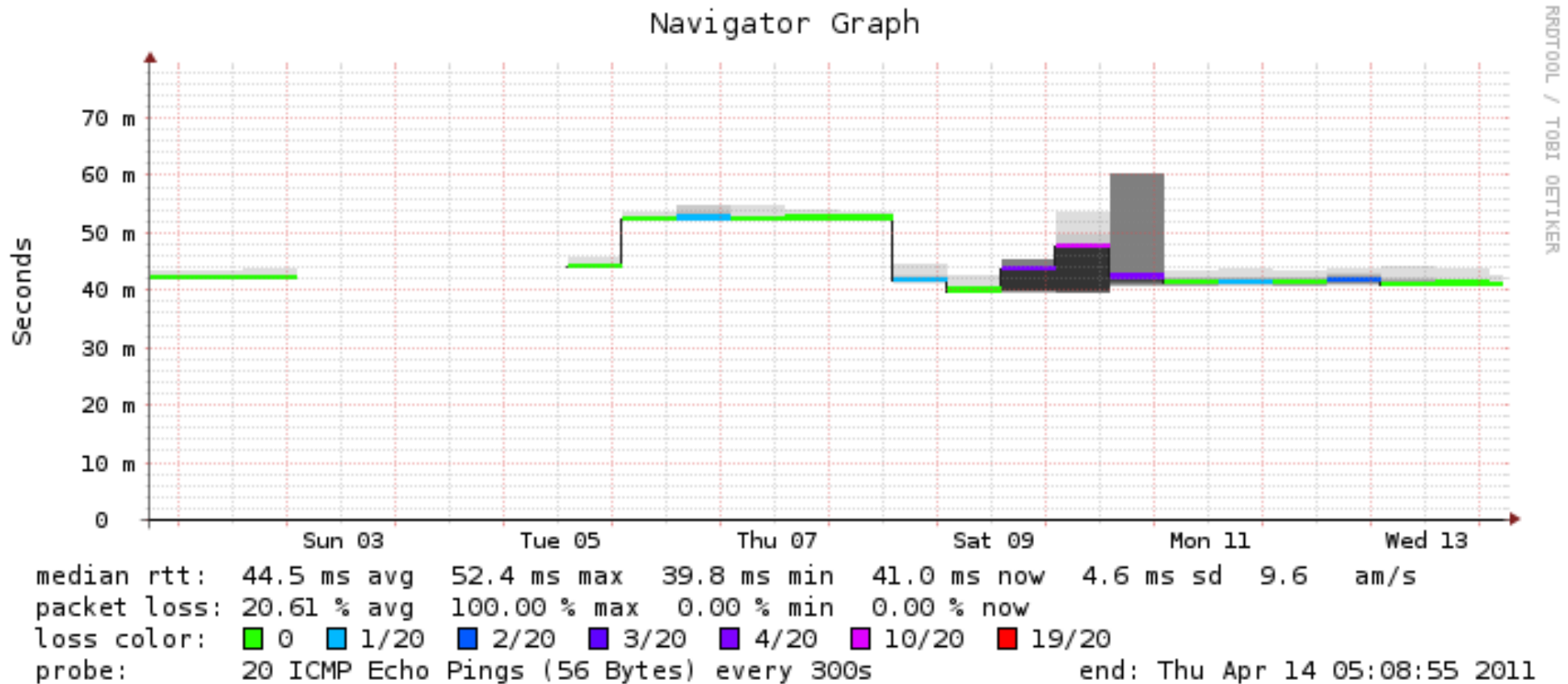
Smokeping

GH_Winneba_Univ_Winneba



Smokeping

IT_Trieste_ICTP



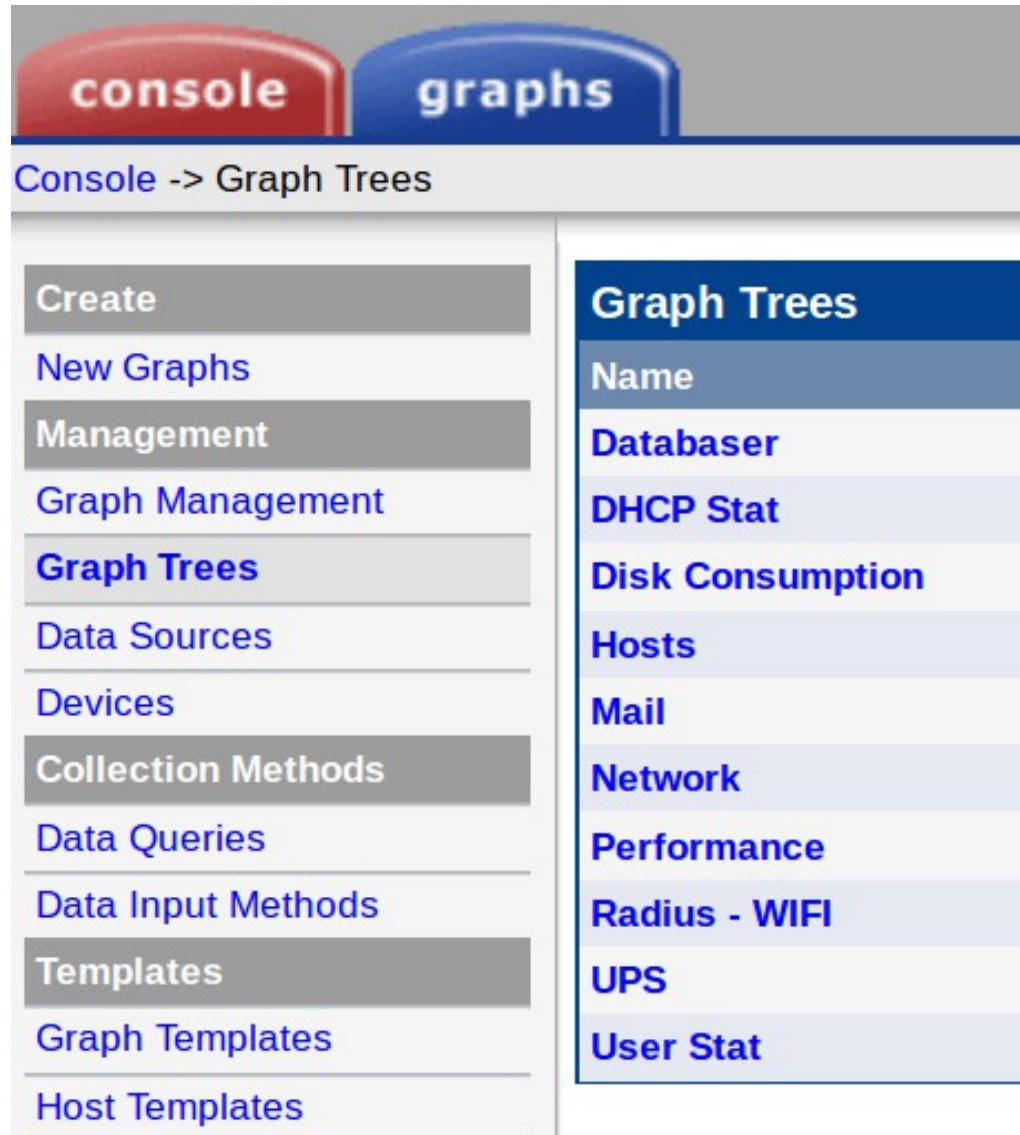
Smokeping – how to get started?

- For example, by using the NSRC exercises:
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/exercises-smokeping-part1.htm>
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/exercises-smokeping-part2.htm>
 - <http://oss.oetiker.ch/smokeping/>

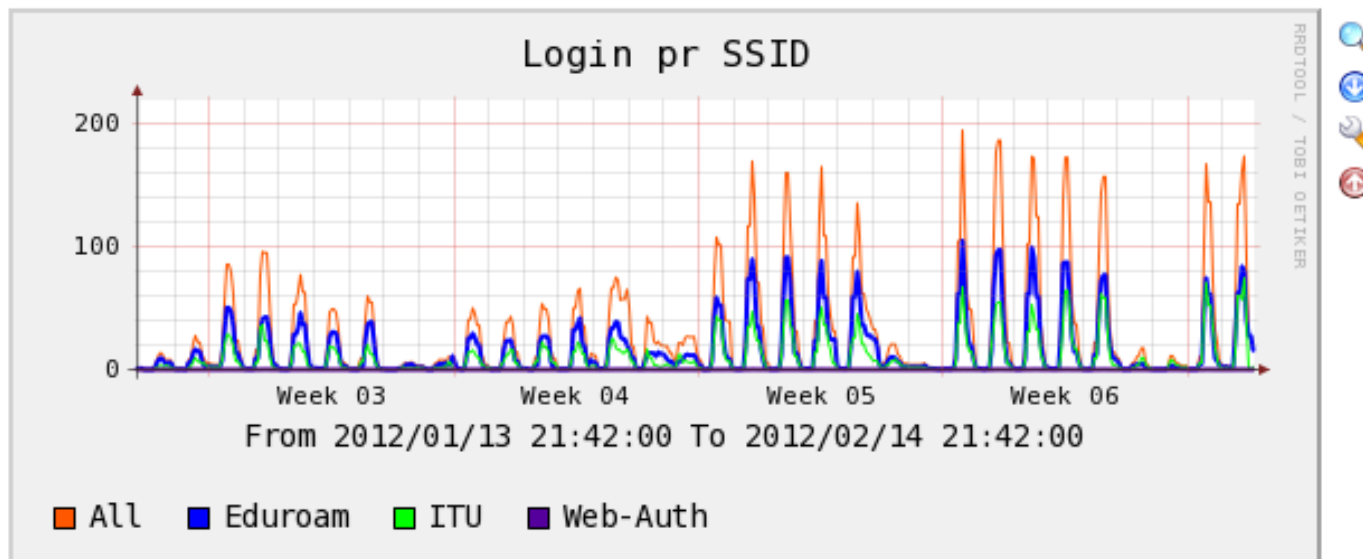
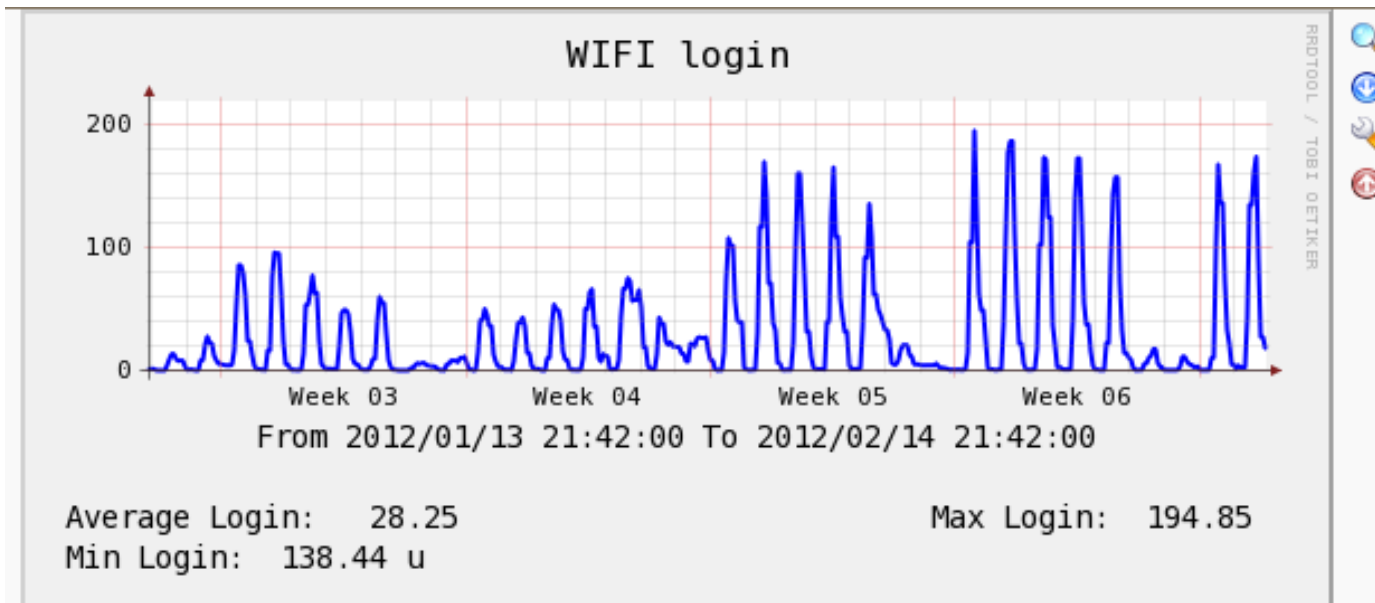
Cacti

- 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)

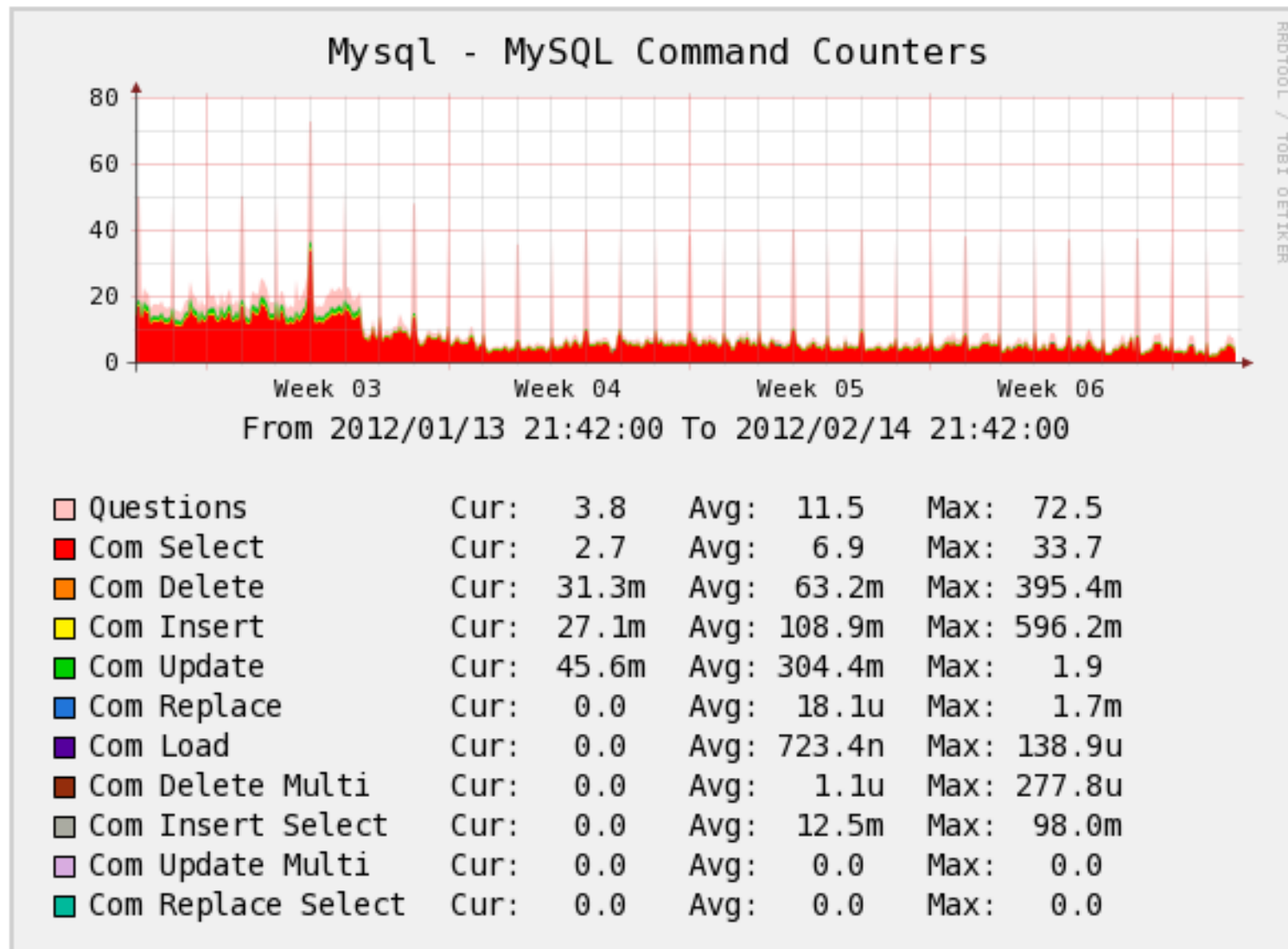
Cacti



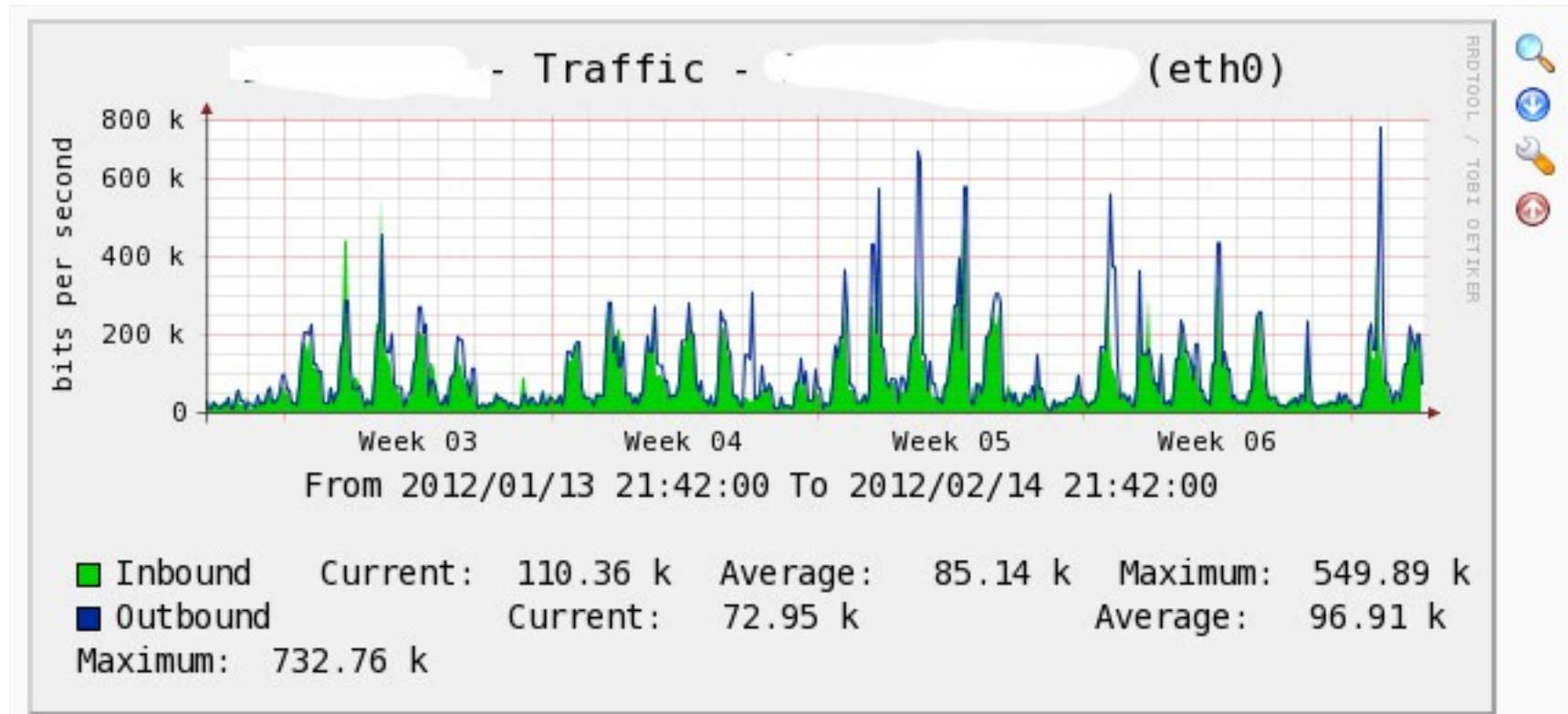
Cacti



Cacti



Cacti



Different types of monitoring



- Cacti is a good tool for:
 - monitoring power, e.g. solar installations as it can monitor electrical and environmental data
 - PoE??? more relevant to Campus...

Cacti – how to get started?

- By now you can guess :)
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/exercises-cacti-part-I.pdf>
 - <https://nsrc.org/workshops/2015/ripe-nsrc-nmm/raw-attachment/wiki/Agenda/cacti-cli-commands.htm>
 - <http://cacti.net>

SNMP

- Simple Network Management Protocol (SNMP)
 - 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."
 - 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.
 - 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

The screenshot shows the Wireshark application window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The main display area is divided into three panes:

- Packet List:** A table showing captured packets. The selected packet (No. 307) is highlighted in green.
- Packet Details:** A tree view showing the hierarchical structure of the selected packet, including Ethernet II, Logical-Link Control, and Data (48 bytes).
- Packet Bytes:** A hex dump and ASCII representation of the packet data.

The status bar at the bottom indicates: wlan0: <live capture in progress> ... Packets: 356 Displayed: 356 Marked: 0

No.	Time	Source	Destination	Protocol	Info
307	10.872327	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
308	10.872407	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=5925 Win=17856 Len=0 TSV=3468518 TSER=451711661
309	10.875996	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
310	10.876065	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=7293 Win=20608 Len=0 TSV=3468519 TSER=451711661
311	10.879649	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
312	10.879722	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=8661 Win=23360 Len=0 TSV=3468520 TSER=451711662
313	10.882863	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
314	10.882945	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=10029 Win=26112 Len=0 TSV=3468521 TSER=451711662
315	10.886785	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
316	10.886856	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=11397 Win=28800 Len=0 TSV=3468522 TSER=451711663
317	10.894122	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]
318	10.894202	140.105.20.155	213.254.17.23	TCP	52920 > http [ACK] Seq=450 Ack=12765 Win=31552 Len=0 TSV=3468524 TSER=451711663
319	10.900093	213.254.17.23	140.105.20.155	TCP	[TCP segment of a reassembled PDU]

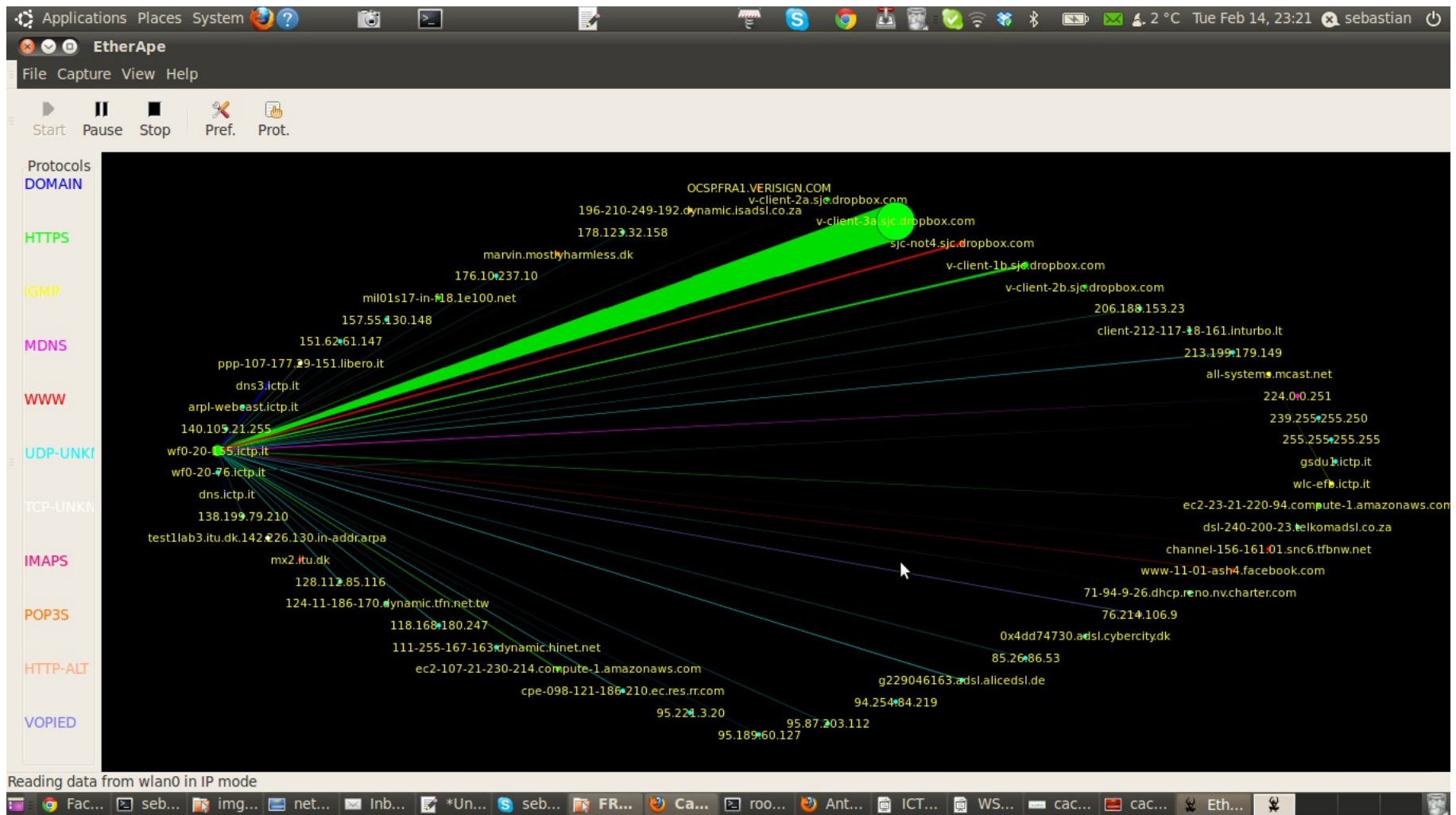
Frame 1 (66 bytes on wire, 66 bytes captured)
+ IEEE 802.3 Ethernet
+ Logical-Link Control
+ Data (48 bytes)

0000 01 0b 85 00 00 00 00 12 d9 b3 26 60 00 34 00 12&`.4..
0010 d9 b3 26 60 aa aa 03 00 0b 85 cc cd 00 1b 00 23 ..&`.... ..#
0020 5e 8a ba 60 00 40 0a 74 00 05 06 01 01 06 06 0a ^...`.t.....
0030 00 00 7f 3b 0f 85 30 40 47 27 79 93 ce 20 ec 0d ...;..0@ G'y..

wlan0: <live capture in progress> ... Packets: 356 Displayed: 356 Marked: 0 Profile: Default

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!