Velkommen til

# Network Management using Mostly Open Source

Henrik Lund Kramshøj
hlk@solidonetworks.com

http://www.solidonetworks.com

Slides are available as PDF

# Goal

*Network and Internet is an integral part of our everyday lives, but how does one ensure that the network works perfectly.*

Introduce essential tools for network management

Prove that open source is critical for network management

Present resources for others to follow

Expect you to be administrators of IP networks, in some way

# Scenario

Presentation is based on the experience from an ISP viewpoint

Walk through of the essential tools and skills you need to acquire

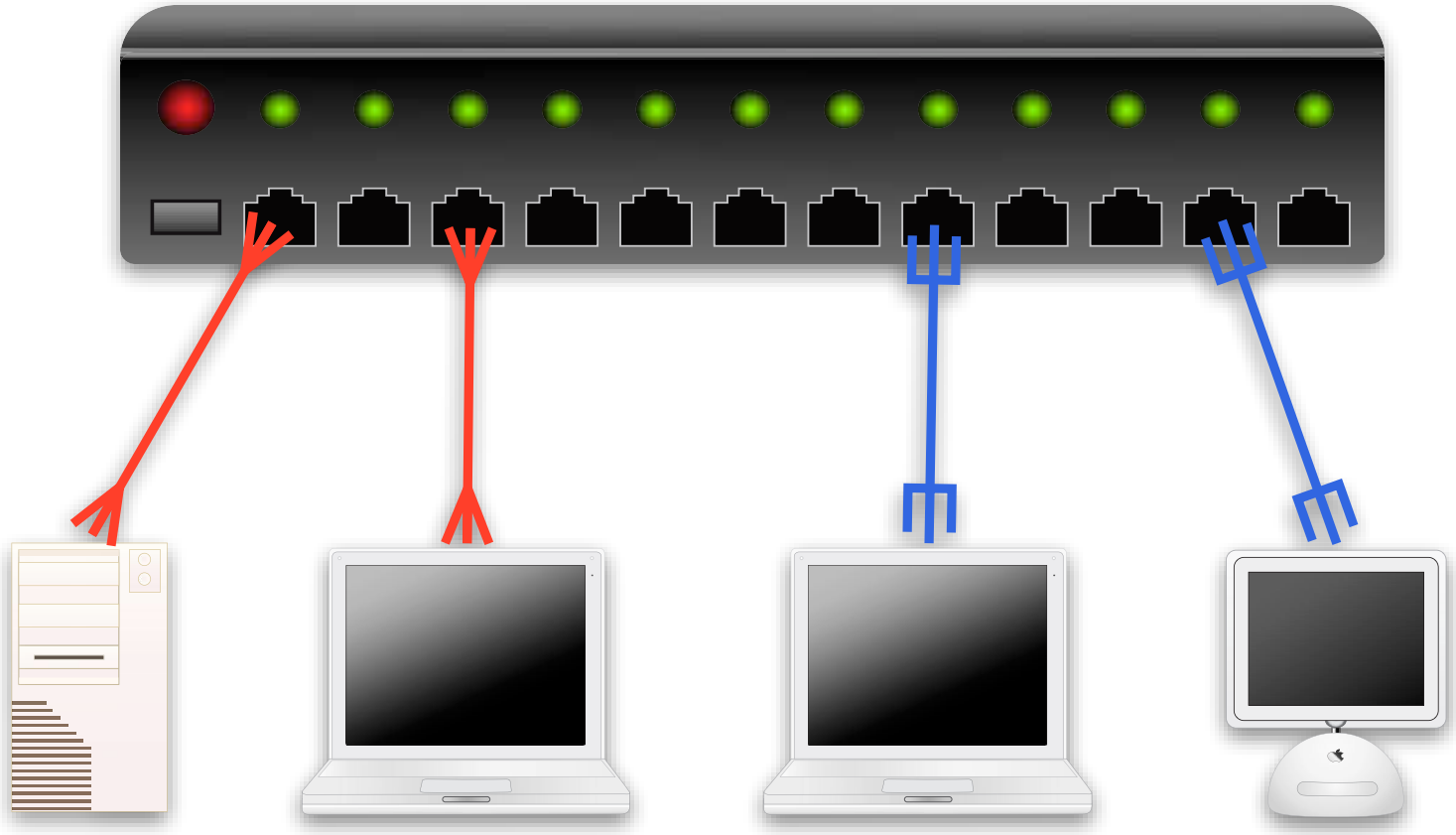
**Contents**

The problem: what is network management

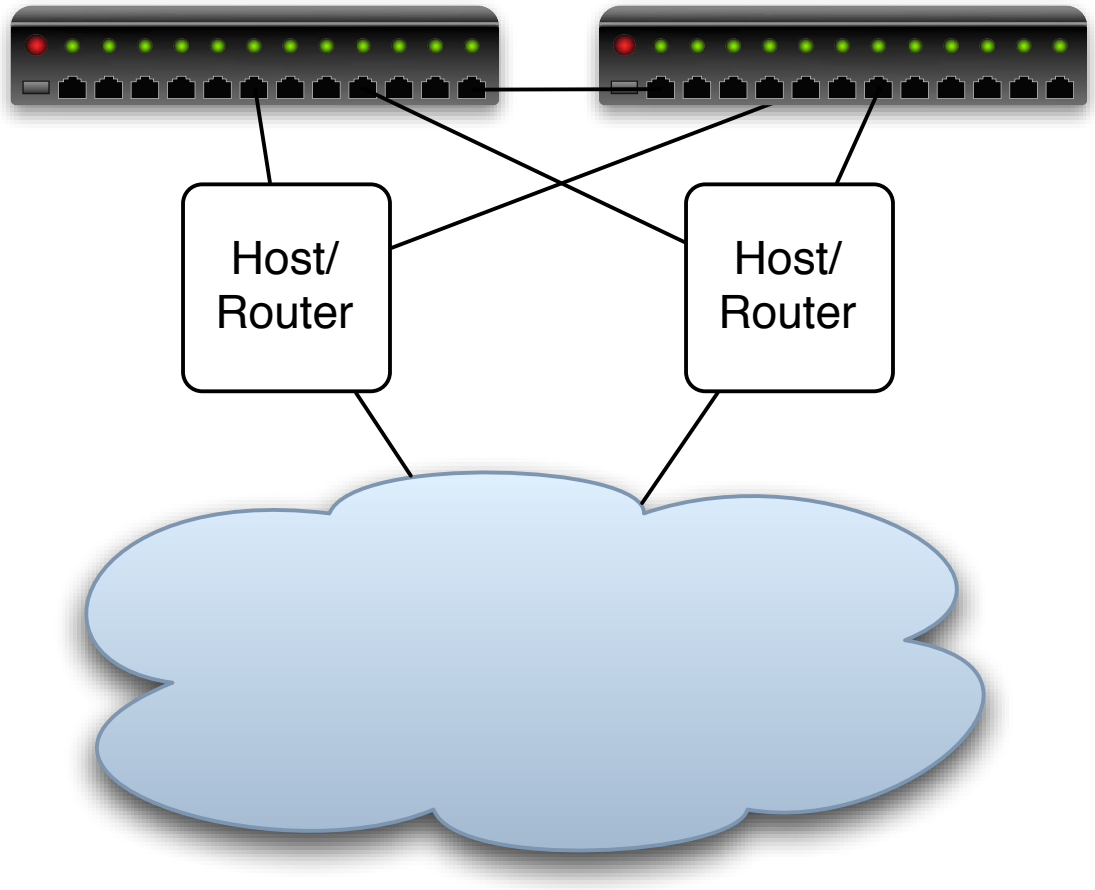
Components of a solution

The solution embrace, extend and proliferate :-)

# The problem: what is network management



# Growing



# Solido Networks AS12617

Core routers at Interxion in Ballerup

Second major site in Luxembourg

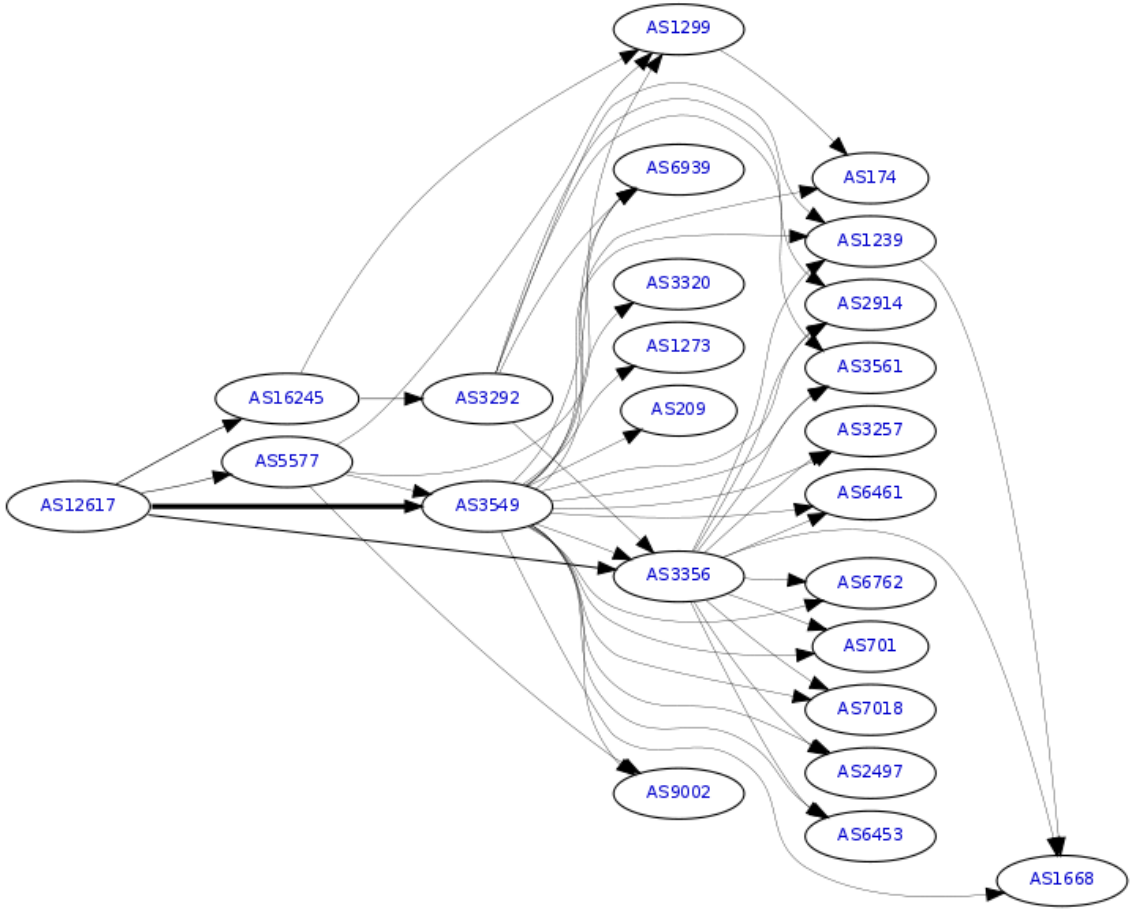
Internet connections multiple 10Gbit at each site

New servers - every week, new switches - every month

Support systems, APC ATS, APC PDU, routers, switches, jump hosts, monitoring, logging servers, support system, ...

**Scheduled down time or outages is not an option anymore**

# AS12617 - high level BGP




Source: `http://bgp.he.net/AS12617`

# Step 1: configure devices properly

SOLIDO NETWORKS

You should always configure your devices properly

Turn on SNMP, probably SNMPv2

Turn on LLDP Link Layer Discovery Protocol,
like CDP but vendor-neutral

`http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol`

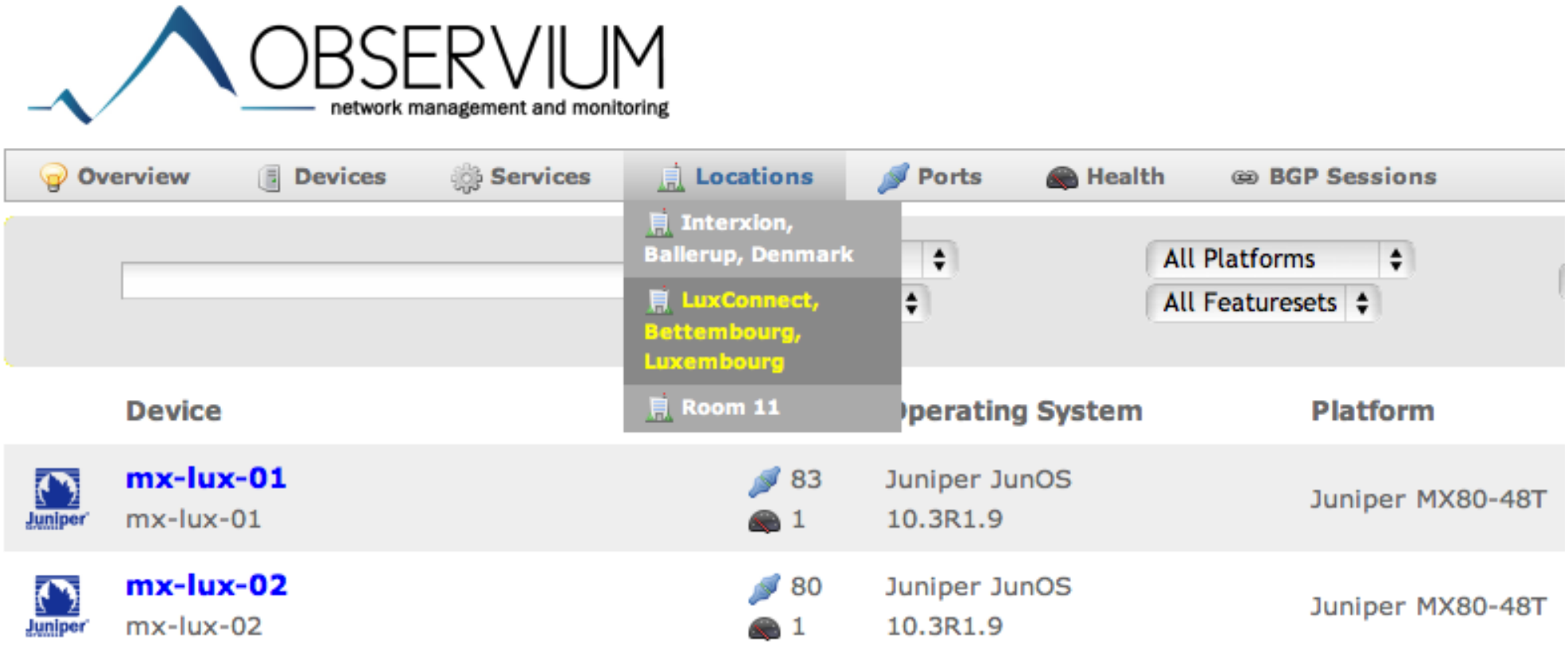
Syslog - you know this, nuff said

And updated firmware, HTTPS and SSH only etc. the usual stuff

# Config example: SNMP

```
snmp {
    description "Solido Networks SRX-CPH-02";
    location "Interxion, Ballerup, Denmark";
    contact "noc@solido.net";
    community yourcommunitynotmine {
        authorization read-only;
        clients {
            10.1.1.1/32;
            10.1.2.2/32;
        }
    }
}
```

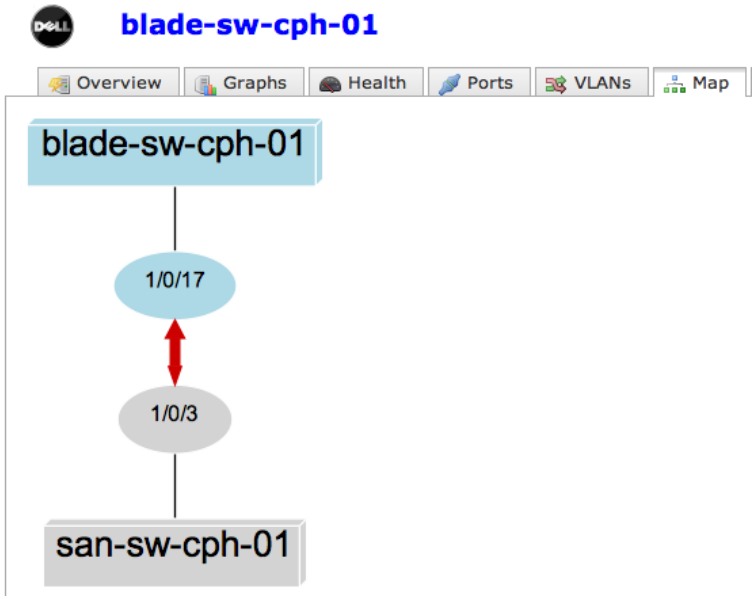
# Location, location, location




Observium picks up the location from SNMP :-)

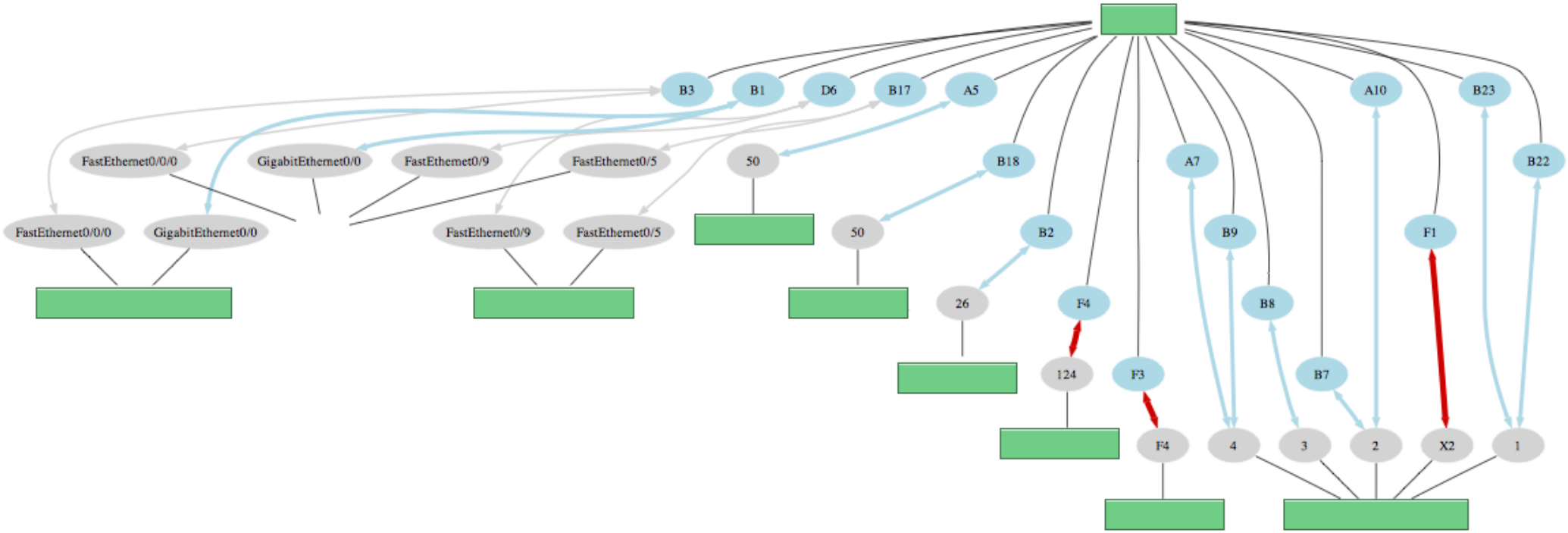
# Config example: LLDP

## Dell 8024F switch LLDP




```
interface ethernet 1/xg17
mtu 9216
lldp transmit-tlv port-desc sys-name sys-desc sys-cap
lldp transmit-mgmt
exit
```

# LLDP spaghetti?




LLDP is needed!

# LLDP trick using tcpdump

```
[hlk@ljh ~]$ sudo tcpdump -i eth0 ether proto 0x88cc
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
.... wait for it ....
11:03:55.395064 00:1c:23:80:49:ff (oui Unknown) > 01:80:c2:00:00:0e (oui Unknown),
ethertype Unknown (0x88cc), length 60:
0x0000:  0207 0400 1c23 8049 fd04 0705 312f 302f  .....#.I....1/0/
0x0010:  3331 0602 0078 0000 0000 0000 0000 0000  31...x..........
0x0020:  0000 0000 0000 0000 0000 0000 0000       ..............

1 packets captured
3 packets received by filter
0 packets dropped by kernel
```

I know **for sure** that this server is in Unit 1 port 31!

# Components of a solution

SOLIDO NETWORKS

*The internet is a collaborative experiment, hippies connecting their routers and liberally exchanging information - sometime money is exchanged also :-)*

Main points, operation, administration, maintenance

Configure your network equipment, provisioning

Monitor your network

Control your network - react to events

Troubleshoot your network

# Learn the basics

Before running in production, and when troubleshooting

Ping and traceroute - you know these, Unix traceroute ICMP/UDP

Nping, Nmap, Mtr, TCP traceroute, hping, icmpush ...

Download Backtrack Linux now, it is your network toolbox
Huge number of goodies on Backtrack for network management!
`http://backtrack-linux.org/`

Learn Unix - yes, Linux/Unix is needed when working with networks
You need skills in sed/awk, cut, **expect**, grep, sort, Perl/Python/Ruby at least one scripting language

# Basic stuff - consoles

SOLIDO NETWORKS

*Conserver is an application that allows multiple users to watch a serial console at the same time. It can log the data, allows users to take write-access of a console (one at a time), and has a variety of bells and whistles to accentuate that basic functionality.*

Watch the console!

A network device rebooted - what happened?

I accidently the whole network, what now?

Serial consoles are not dead, and still very useful

`http://www.conserver.com/`

# Hardware and software


Soekris, 4-port serial card EUR59 / 430DKK + OpenBSD + conserver

# Conserver is easy

```
### set the defaults for all the consoles
# these get applied before anything else
default * {
        # The '&' character is substituted with the console name
        logfile /var/consoles/&;
        # timestamps every hour with activity and break logging
        timestamp 1hab;
        # include the 'full' default
        include full;
        # master server is localhost
        master localhost;
}
...
console portS1 {
        type device;
        device /dev/cua02; parity none; baud 57600;
        idlestring "#";
        idletimeout 5m;         # send a '#' every 5 minutes of idle
        timestamp "";           # no timestamps on this console
}
```

You will actually be able to say what happened at that device

# Monitor your network

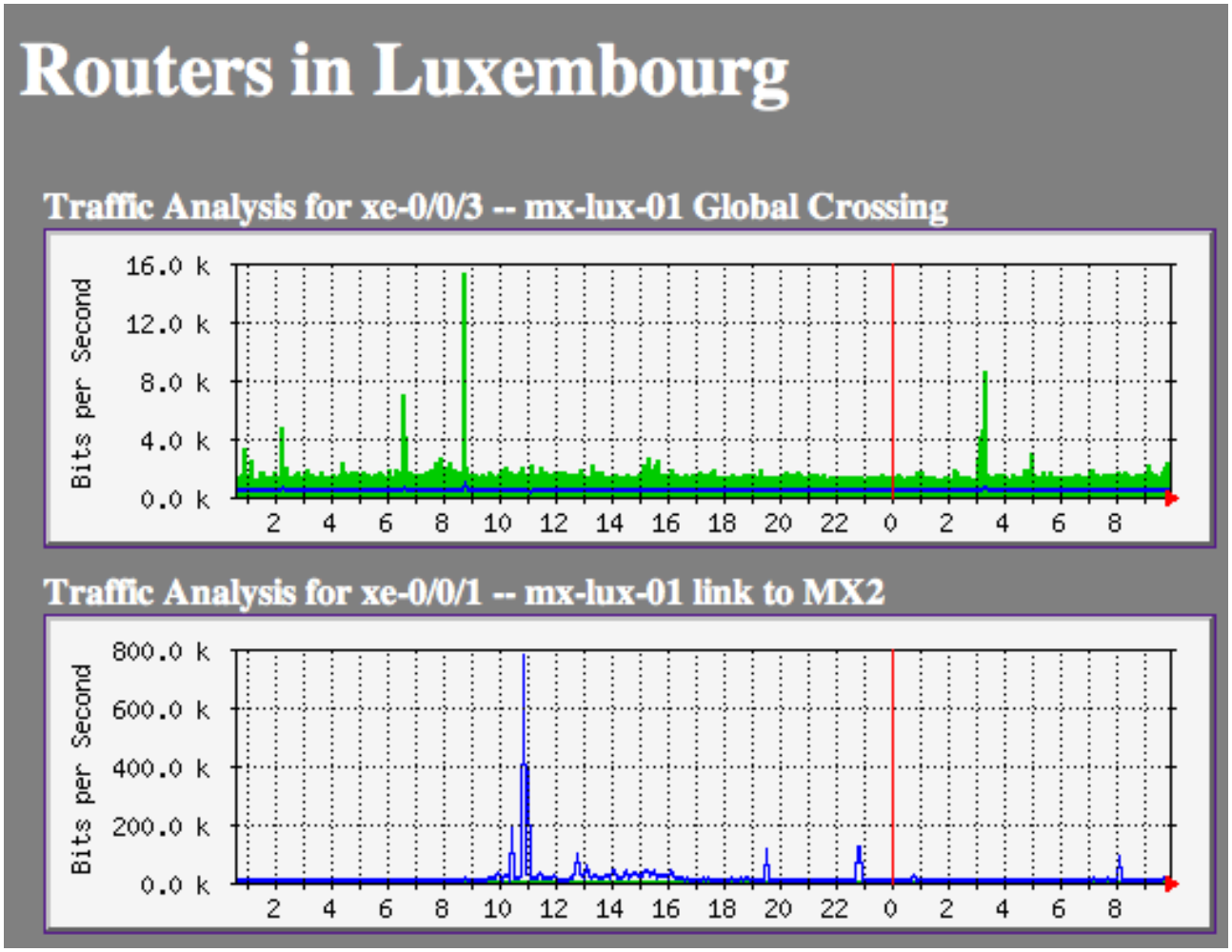
MRTG The Multi Router Traffic Grapher - simple, great, fast
`http://oss.oetiker.ch/mrtg/`

Smokeping Network Latency measurements - network quality
`http://oss.oetiker.ch/smokeping/`

NFsen Netflow monitoring - turn on at selected routers/switches

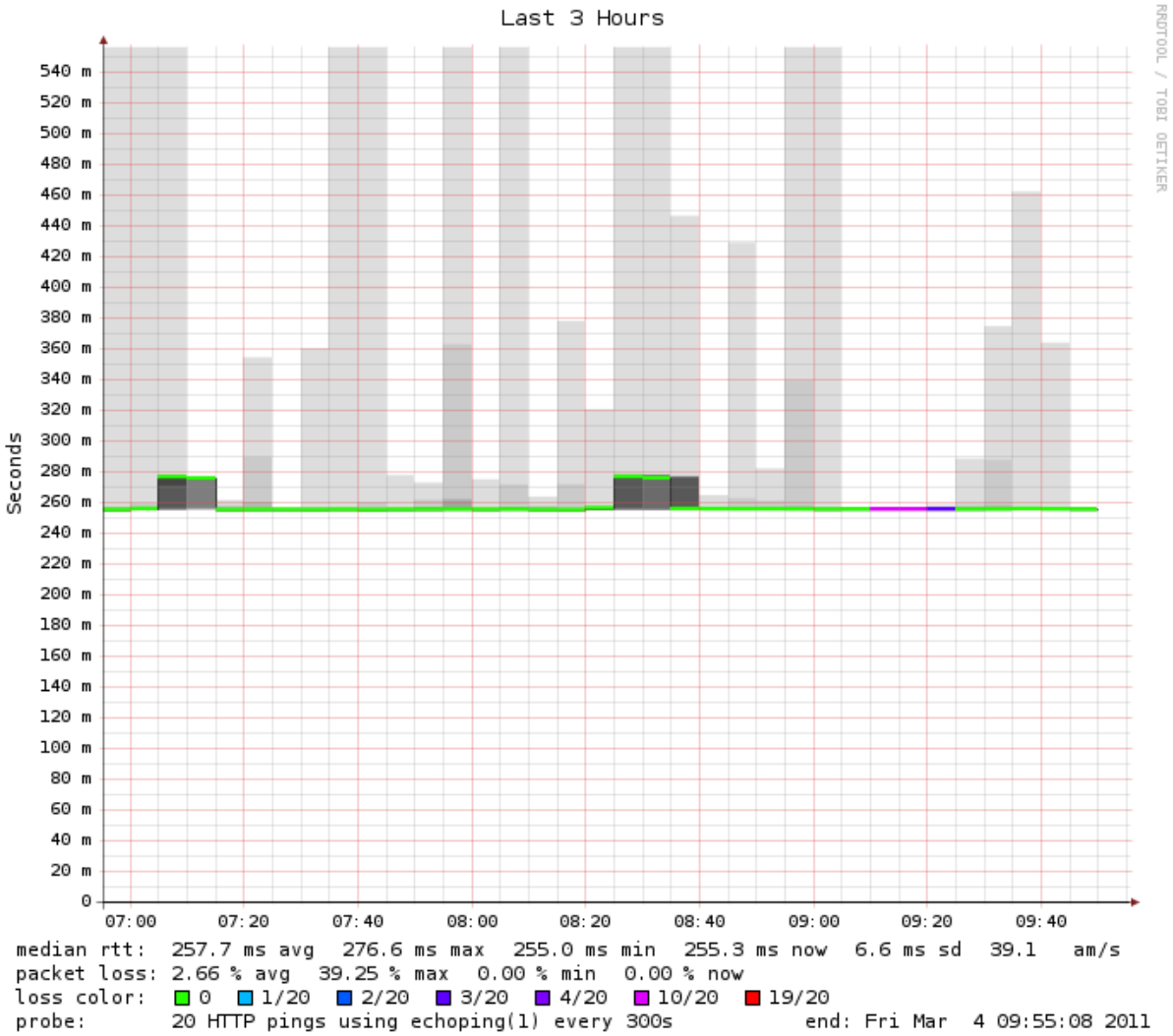
Manual tools, My Traceroute, Nping

# MRTG SNMP monitoring made easy




Run configmaker, indexmaker - almost done

# Smokeping packet loss



# Smokeping latency changed

# Netflow

SOLIDO NETWORKS

Netflow is getting more important, more data share the same links

Accounting is important

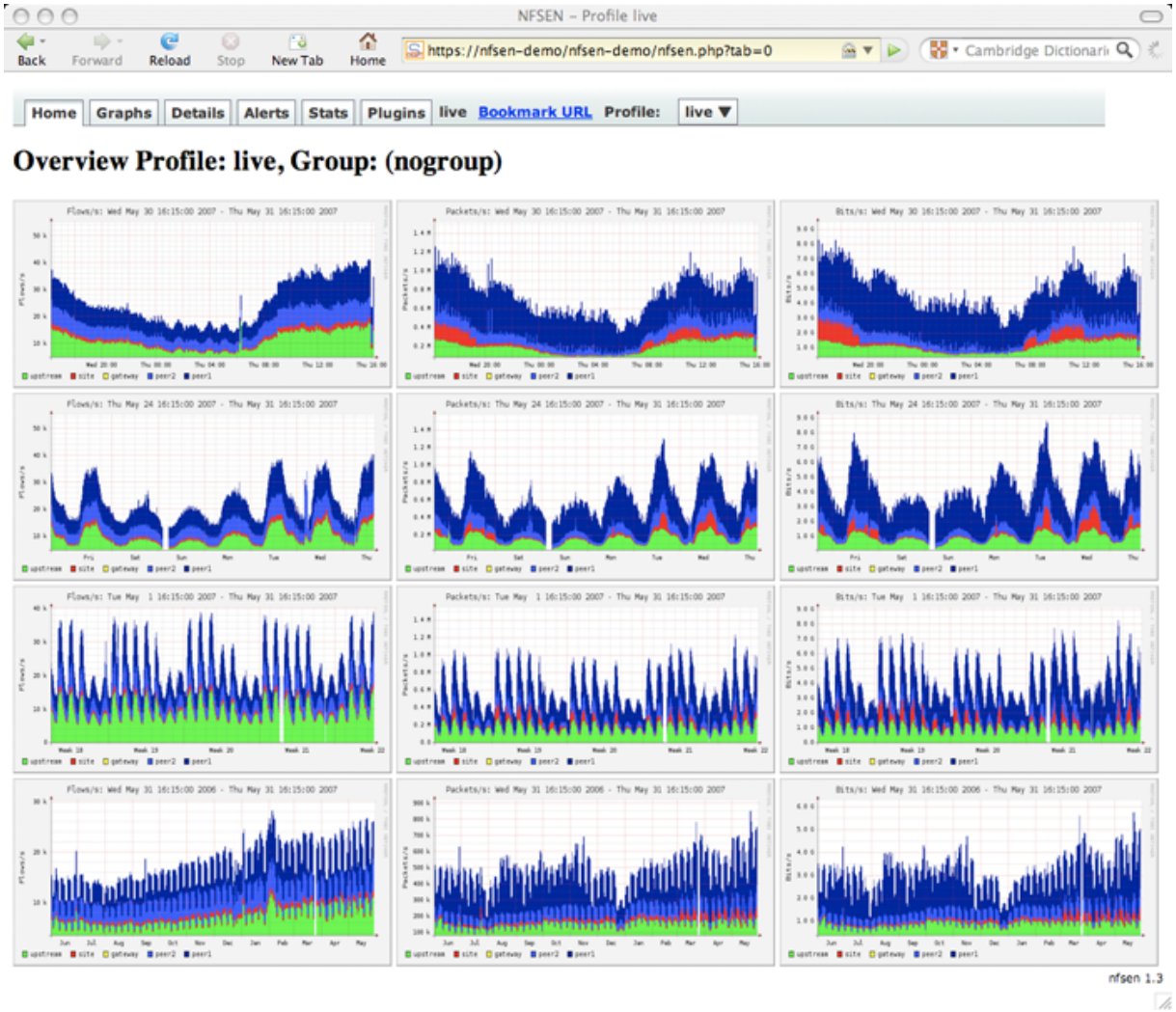
Detecting DoS/DDoS and problems is essential

Netflow sampling is vital information - 123Mbit, but what kind of traffic

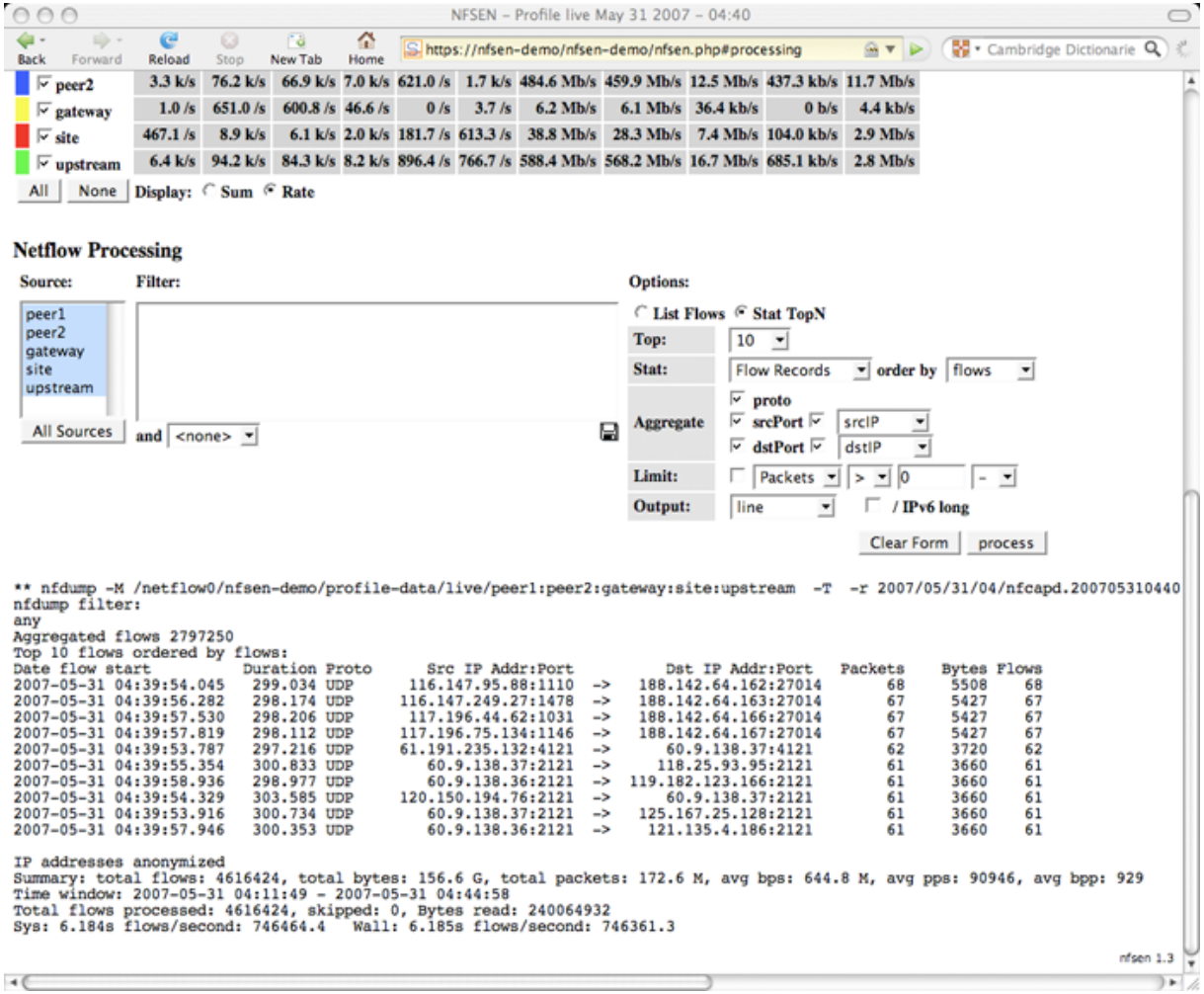
We use mostly NFSen, but are looking at various software packages `http://nfsen.sourceforge.net/`

Currently also investigating sFlow - hopefully more fine grained

# Netflow using NFSen



# Netflow processing from the web interface




Bringing the power of the command line forward

# My Traceroute

```
                                                My traceroute  [v0.74]
pumba.kramse.dk (::)                                          Fri Mar  4 10:22:08 2011
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                   Packets               Pings
 Host                                             Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 2001:16d8:dd0e:1::100                          0.0%     7    0.1   0.1   0.1   0.1   0.0
 2. gw-26.cph-01.dk.sixxs.net                      0.0%     6   13.7  13.7  13.6  13.9   0.1
 3. 3229-sixxs.cr0-r72.gbl-cph.dk.ip6.p80.net      0.0%     6   14.3  14.3  14.3  14.4   0.0
 4. te4-3-r72.cr0-r70.tc2-ams.nl.ip6.p80.net       0.0%     6   25.4  51.0  25.3 178.6  62.5
 5. 20gigabitethernet1-3.core1.ams1.ipv6.he.net    0.0%     6   25.8  26.5  25.7  29.9   1.7
 6. ge-0.ams-ix.amstnl02.nl.bb.gin.ntt.net         0.0%     6   26.3  32.0  26.3  60.2  13.8
 7. as-0.r25.tokyjp01.jp.bb.gin.ntt.net            0.0%     6  284.1 306.1 283.6 372.8  37.1
 8. po-2.a15.tokyjp01.jp.ra.gin.ntt.net            0.0%     6  298.4 298.3 298.1 298.5   0.2
 9. ge-8-2.a15.tokyjp01.jp.ra.gin.ntt.net          0.0%     6  301.2 301.2 300.9 301.7   0.3
10. ve44.foundry6.otemachi.wide.ad.jp              0.0%     6  300.9 300.9 300.8 301.0   0.1
11. ve42.foundry4.nezu.wide.ad.jp                  0.0%     6  301.0 301.0 300.9 301.3   0.2
12. cloud-net1.wide.ad.jp                          0.0%     6  301.1 301.0 300.9 301.1   0.1
13. 2001:200:dff:fff1:216:3eff:feb1:44d7           0.0%     6  301.3 301.2 301.0 301.3   0.1
```

# Nping new kid on the block

```
hlk@pumba:nmap-5.51$ nping www.solidonetworks.com

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0059s) Starting TCP Handshake > www.solidonetworks.com:80 (91.102.95.20:80)
RECV (0.0067s) Handshake with www.solidonetworks.com:80 (91.102.95.20:80) completed
SENT (1.0093s) Starting TCP Handshake > www.solidonetworks.com:80 (91.102.95.20:80)
RECV (1.0105s) Handshake with www.solidonetworks.com:80 (91.102.95.20:80) completed
SENT (2.0193s) Starting TCP Handshake > www.solidonetworks.com:80 (91.102.95.20:80)
RECV (2.0201s) Handshake with www.solidonetworks.com:80 (91.102.95.20:80) completed
SENT (3.0293s) Starting TCP Handshake > www.solidonetworks.com:80 (91.102.95.20:80)
RECV (3.0302s) Handshake with www.solidonetworks.com:80 (91.102.95.20:80) completed
SENT (4.0393s) Starting TCP Handshake > www.solidonetworks.com:80 (91.102.95.20:80)
RECV (4.0402s) Handshake with www.solidonetworks.com:80 (91.102.95.20:80) completed

Max rtt: 1.193ms | Min rtt: 0.781ms | Avg rtt: 0.932ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.03457s | Tx bytes/s: 99.14 | Tx pkts/s: 1.24
Rx time: 4.03550s | Rx bytes/s: 49.56 | Rx pkts/s: 1.24
Nping done: 1 IP address pinged in 4.04 seconds
```

# Nping is sexy too

```
hlk@pumba:nmap-5.51$ nping -6  www.solidonetworks.com

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0061s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (0.0224s) Handshake with 2a02:9d0:10::9:80 completed
SENT (1.0213s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (1.0376s) Handshake with 2a02:9d0:10::9:80 completed
SENT (2.0313s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (2.0476s) Handshake with 2a02:9d0:10::9:80 completed
SENT (3.0413s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (3.0576s) Handshake with 2a02:9d0:10::9:80 completed
SENT (4.0513s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (4.0678s) Handshake with 2a02:9d0:10::9:80 completed

Max rtt: 16.402ms | Min rtt: 16.249ms | Avg rtt: 16.318ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.04653s | Tx bytes/s: 98.85 | Tx pkts/s: 1.24
Rx time: 4.06292s | Rx bytes/s: 49.23 | Rx pkts/s: 1.23
Nping done: 1 IP address pinged in 4.07 seconds
```

Are you running IPv6?
Please do not buy devices or connections without asking for IPv6!

# Control your network

SOLIDO NETWORKS

RANCID - Really Awesome New Cisco conflg Differ
+ Juniper, Dell, ... `http://www.shrubbery.net/rancid/`

Expect, script etc. great for installing devices with common settings
`http://expect.sourceforge.net/` the expect home page

Self discovering: Observium, new and not perfect, but very useful

# RANCID

```
[rancid@ljh routers]$ cat router.db
mx-lux-01:juniper:up
mx-lux-02:juniper:up
...
[rancid@ljh routers]$ crontab -l
# run config differ hourly
07 0-23/2 * * * /usr/local/rancid/bin/rancid-run
# clean out config differ logs
50 23 * * * /usr/bin/find /usr/local/rancid/var/logs -type f -mtime +2 -exec rm {}
```

RANCID will then fetch configurations, and more, and put it into version control SVN/CVS

Changes are emailed to an email alias

# RANCID output

carrier-switches router config diffs — RANCID

From: rancid@l[redacted]
Subject: **carrier-switches router config diffs**
Date: 19. jan 2011 02.09.28 CET
To: rancid-carrier-switches@l[redacted]

```
Index: configs/c1-cph-01
===================================================================
- -- configs/c1-cph-01  (revision 1457)
@@ -210,7 +210,7 @@
 exit
 !
 interface ethernet 1/g45
- description 'SRX240'
+ description 'SRX-CPH-02 ge-0/0/0'
 switchport mode general
 switchport general allowed vlan add 95,3000-3005 tagged
 exit
```

# RANCID hints

SUBVERSION REPOSITORIES RANCID

English - English

(root)/san-switches/configs/san-sw-cph-01 - Rev 1608

Rev HEAD Go

Rev 1600 | Blame | Compare with Previous | Last modification | View Log | Download | RSS feed

```
!RANCID-CONTENT-TYPE: Dell
!
!
Image Descriptions
 image1 : default image
 image2 :
 Images currently available on Flash
-----------------------------------------------------------------
 unit      image1      image2     current-active        next-active
-----------------------------------------------------------------
```

Hints:

Use rancid user on server and devices, preferably read-only

Use SSH keys to avoid clear text passwords in `~rancid/.cloginrc`

Expose the Subversion to others in the organization using websvn

# Expect

SOLIDO NETWORKS

*Me: Why does it take that long to change this setting?*
*Them: Because we log into each router manually*

RANCID uses Expect, for example in the clogin script

Using the clogin script it is possible to perform a command on - say 60 routers in less than 10 minutes ...

Sure, you should watch over the process, but typing your loooong and complex network password 60 times?!

**Are you fucking mental?!**

# Expect example - clogin from RANCID

```
expect {
    -re "(Connection refused|Secure connection \[^\n\r]+ refused)" {
        catch {close}; catch {wait};
        if !$progs {
            send_user "\nError: Connection Refused ($prog): $router\n"
            return 1
        }
    }
    -re "(Connection closed by|Connection to \[^\n\r]+ closed)" {
        catch {close}; catch {wait};
        if !$progs {
            send_user "\nError: Connection closed ($prog): $router\n"
            return 1
        }
    }
    -re "(Host key not found |The authenticity of host .* be established).*\(yes\/no\)\?" {
        send "yes\r"
        send_user "\nHost $router added to the list of known hosts.\n"
        exp_continue
    }
```

# Observium

*Observium is an autodiscovering PHP/MySQL based network monitoring system focused primarily on Cisco and Linux networks but includes support for a wide range of network hardware and operating systems.*

Tested it at The Camp summer 2010 not ready

Tested it again Fall 2010, not finished, but useful enough

`http://observium.org/`

Easy up and running

`http://www.observium.org/wiki/CentOS_SVN_Installation`

# Why makes Observium great?

```
[root@wiseguy observium]# ./addhost.php
Add Host Tool
Usage: ./addhost.php <hostname> [community] [v1|v2c] [port]
```

Configure your devices in a consistent way

Add host and discover the rest using Observium - done

Surf your network data, including BGP sessions

# Observium example router overview

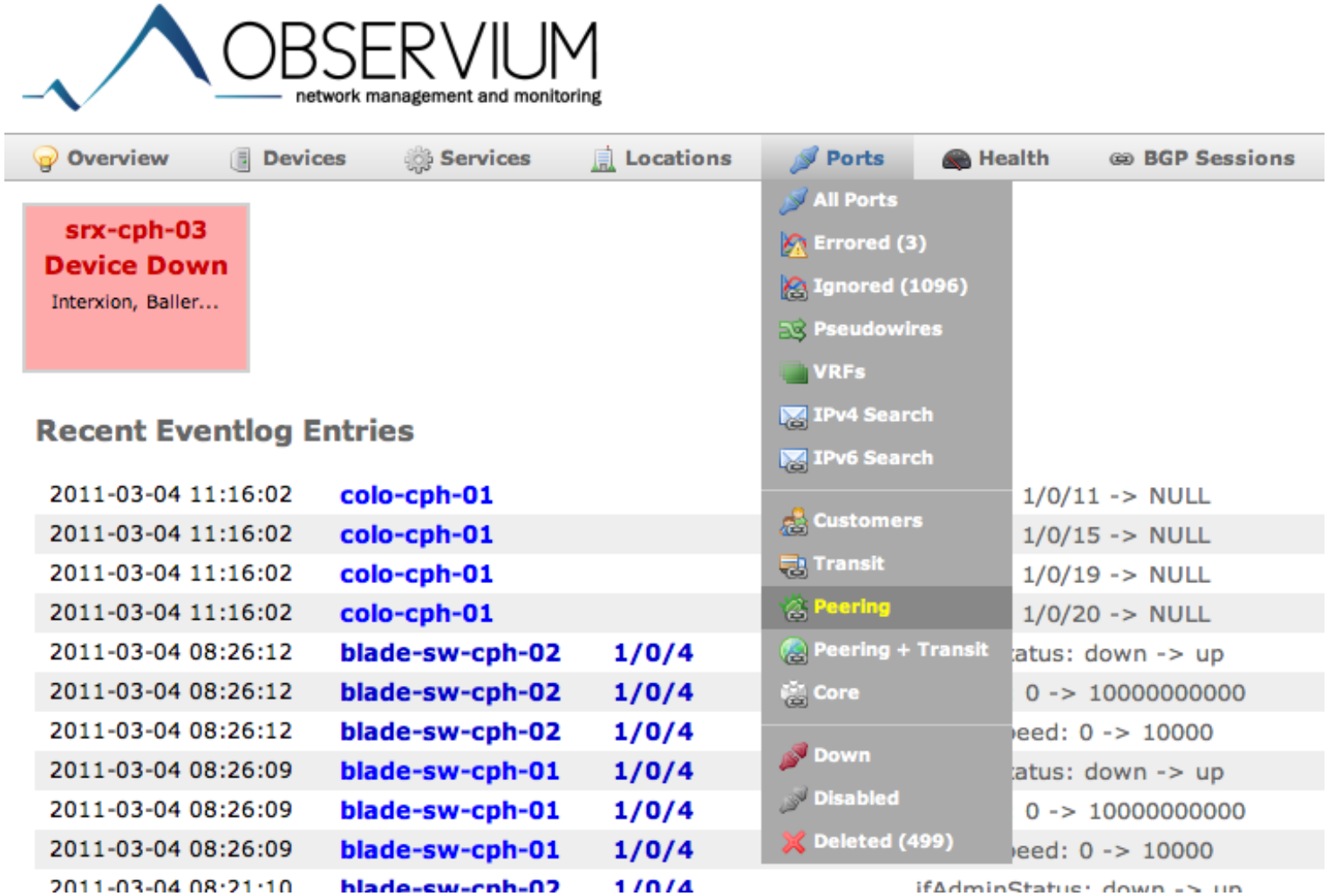

More useful information than default vendor interface! (flash)

# Sort customers and transit

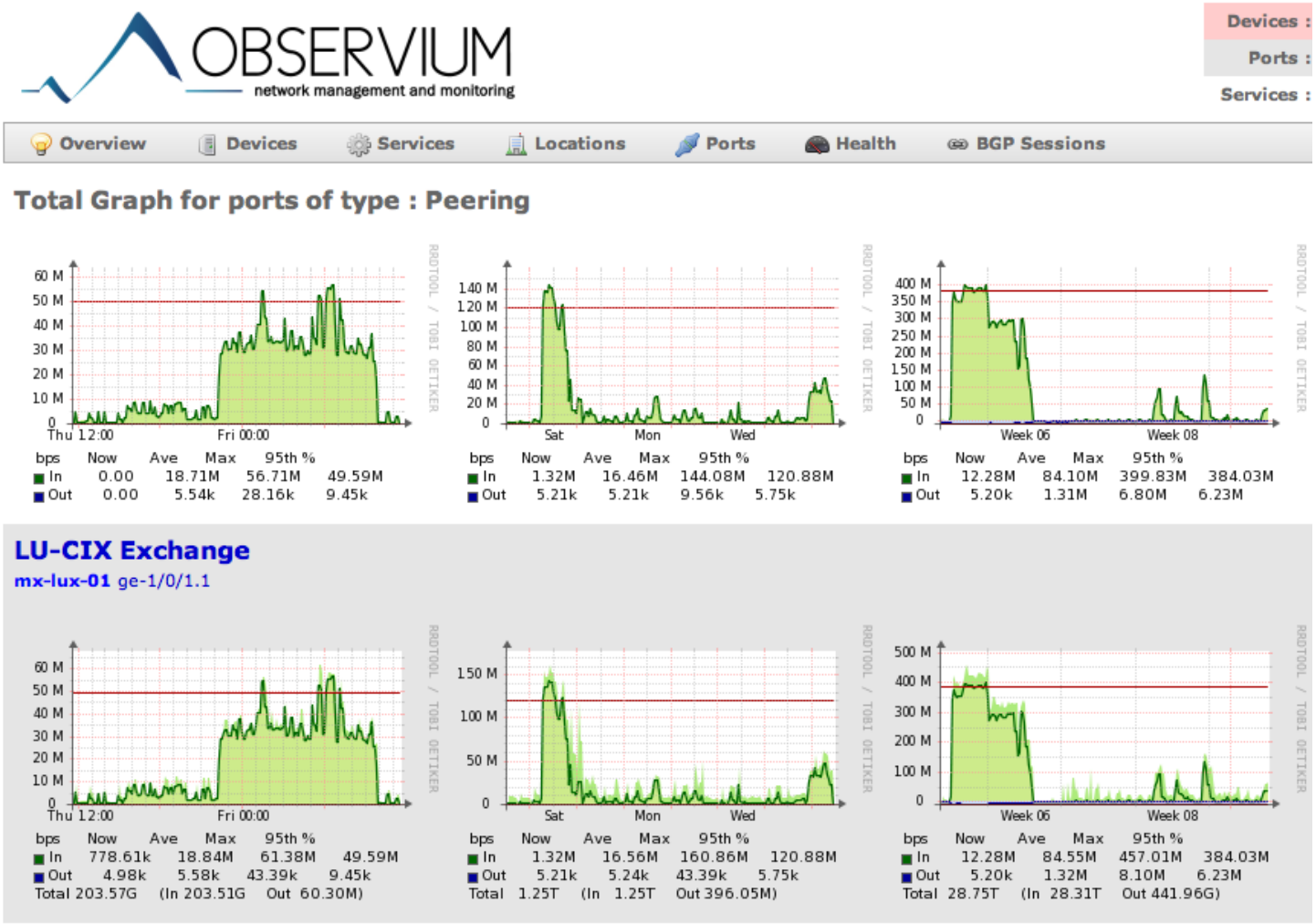
```
--- JUNOS 9.6R2.11 built 2009-10-06 20:09:34 UTC
hlk@ ...> show configuration interfaces
...
xe-2/0/0 {
    description "Transit: Netgroup (AS16245)";
...
ge-4/0/0 {
    description "Cust: xxx (200Mbit contract)";

Another router:
ge-1/0/1 {
    unit 0 {
        description "Peering: LU-CIX Exchange";
```

http://www.observium.org/wiki/Interface_Description_Parsing

# Overview ports

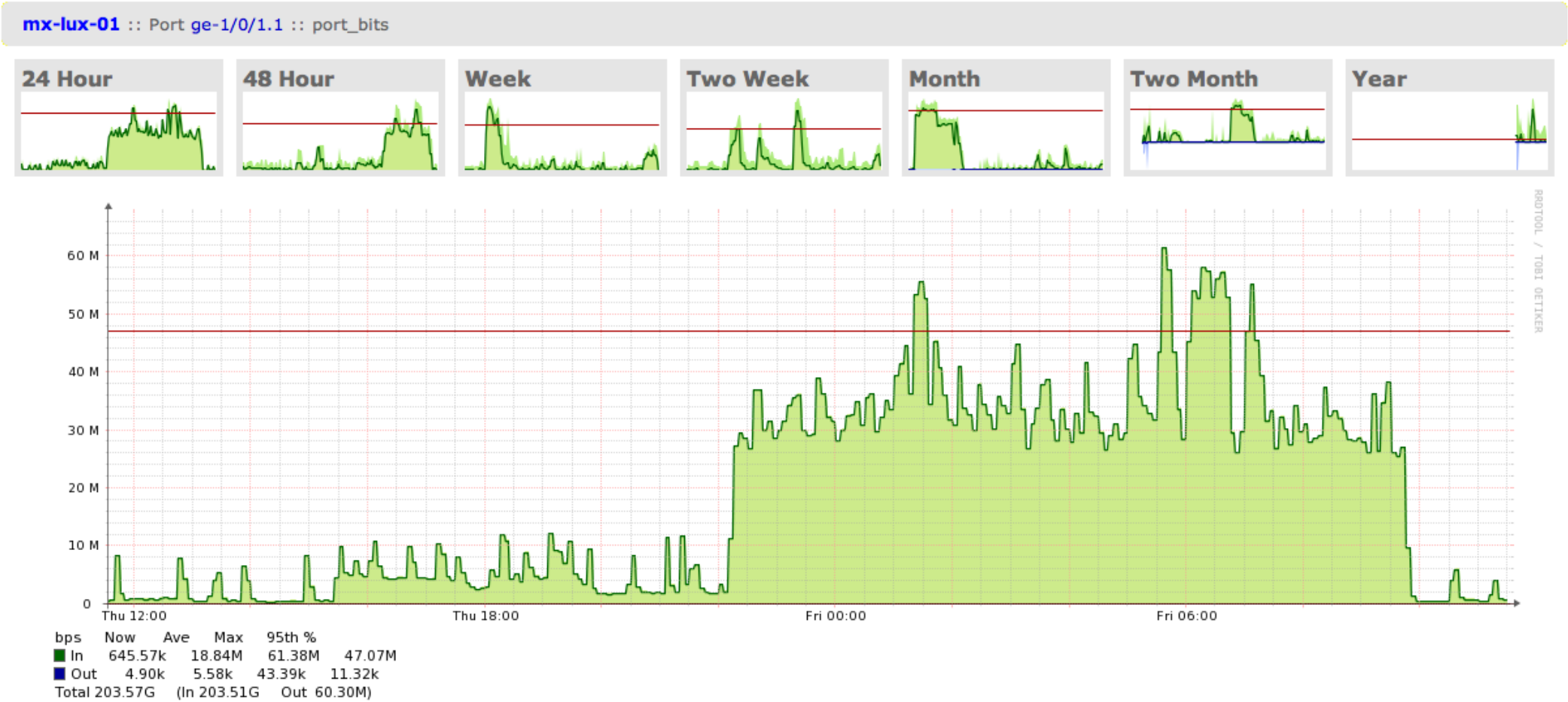


# Overview peering ports



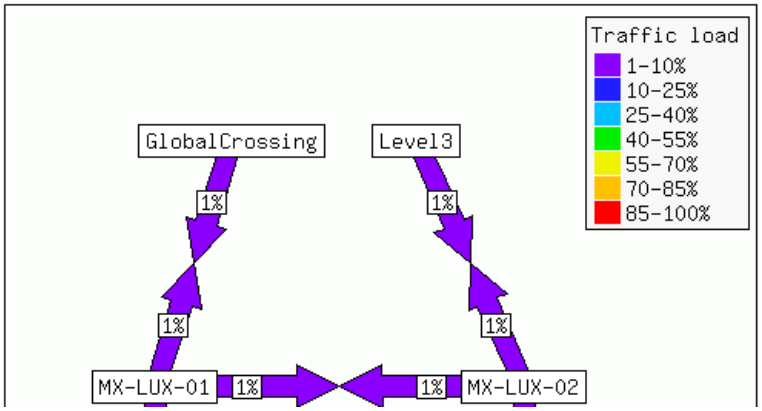

(does not show all peerings we have)

# Overview ports




Drill down and hyperlinks everywhere

# Combine tools




Reuse data - google: mrtg weathermap will show multiple tools

We use: `http://netmon.grnet.gr/weathermap/`

Many tools use RRDtool - recreate specific graphs

Gather links and create overview pages with the most important ones

A virtual NOC with Open Source IMHO better than any commercial tool

# Embrace, extend and proliferate

SOLIDO NETWORKS

We have shown a number of high quality tools

Use them and keep the flame burning

Open Source is critical and we need more network skills

# Web sites for network management

Dont forget about the nice websites that work to your advantage:

Routing Information Service and Whois
`http://www.ripe.net`

traceroutes to your network
`http://www.traceroute.org`

`http://nanog.cluepon.net/index.php/Tools_and_Resources`

`http://labs.ripe.net/Members/vastur/the-shape-of-a-bgp-update`

`http://www.delicious.com/kramshoej/netflow` and other tags

And use google :-)

# Questions?

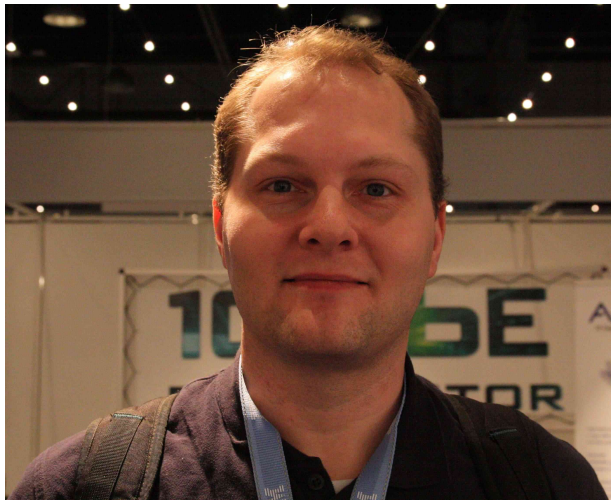
Henrik Lund Kramshøj
hlk@solidonetworks.com

http://www.solidonetworks.com

You are always welcome to send me questions later via email

**Networks tools are here already - use them**

# Contact information



- Henrik Lund Kramshøj, IT-security and IP network consultant
- Email: hlk@solidonetworks.com Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP and CEH certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS