SOLIDO NETWORKS

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

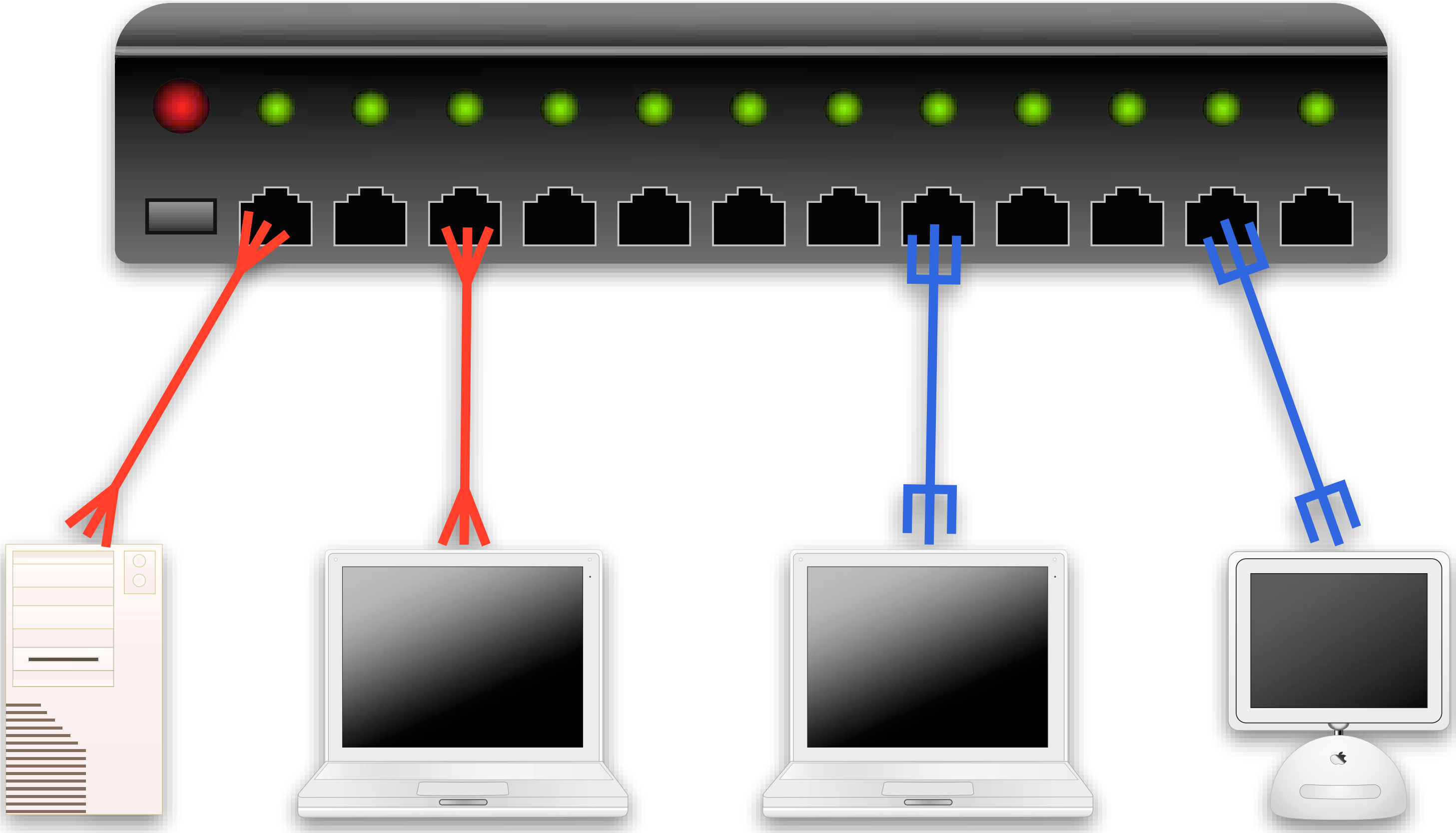
**Contents**

The problem: what is network management

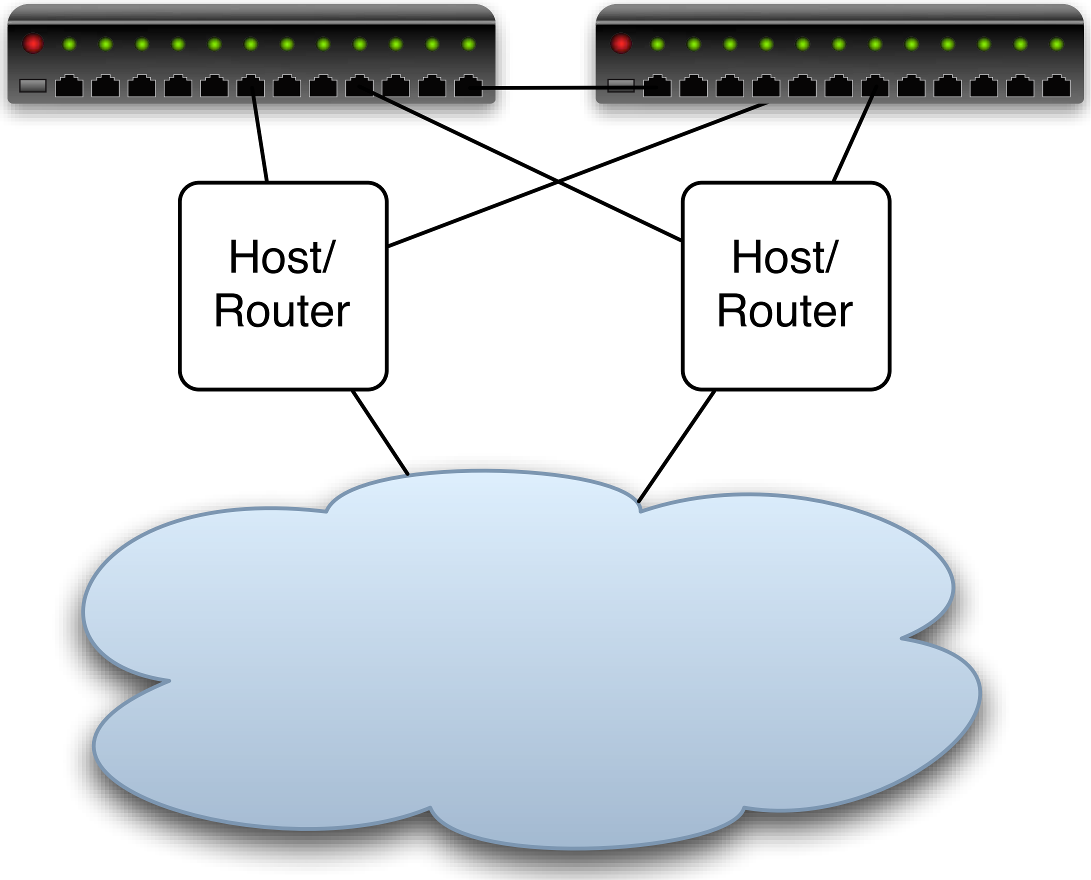
Components of a solution

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

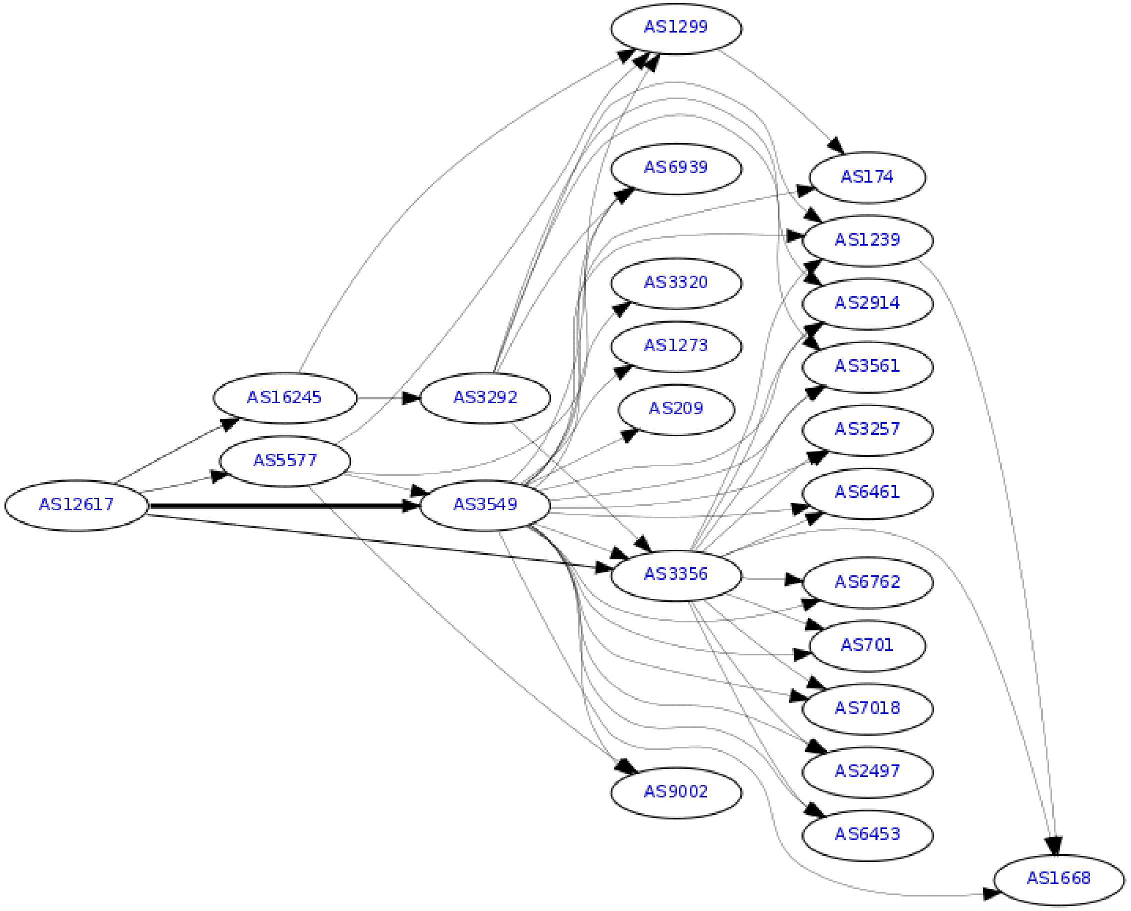
Internet connections multiple 10Gbit at each site

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

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`

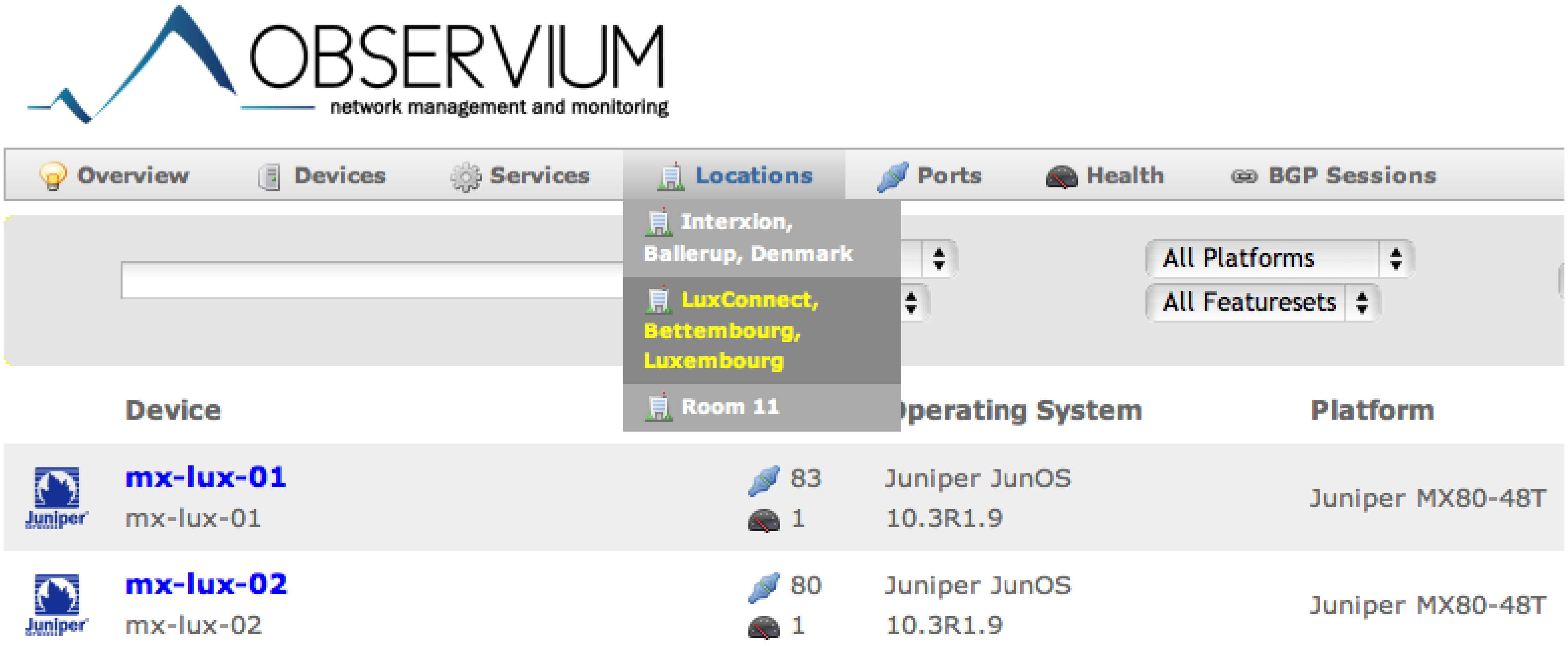
Syslog - you know this, nuff said

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

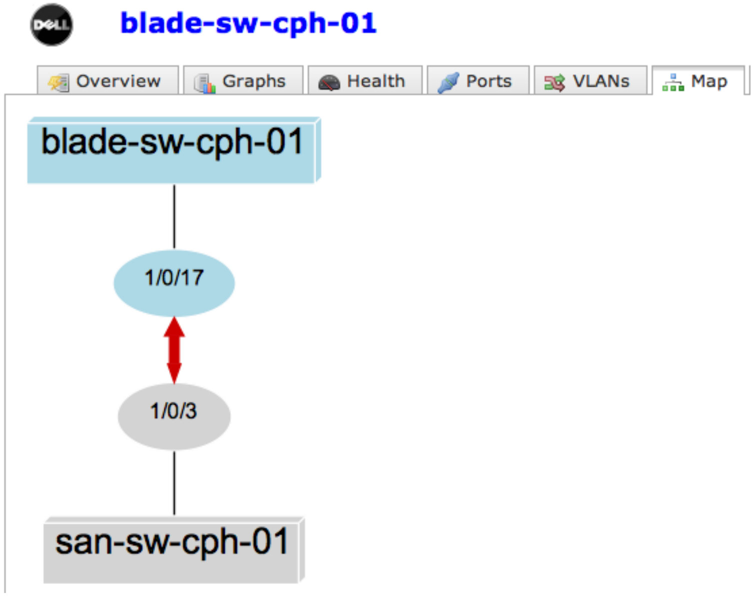


| Device | | perating System | Platform |
|---|---|---|---|
| mx-lux-01<br>mx-lux-01 | 83<br>1 | Juniper JunOS<br>10.3R1.9 | Juniper MX80-48T |
| mx-lux-02<br>mx-lux-02 | 80<br>1 | Juniper JunOS<br>10.3R1.9 | Juniper MX80-48T |

Observium picks up the location from SNMP :-)

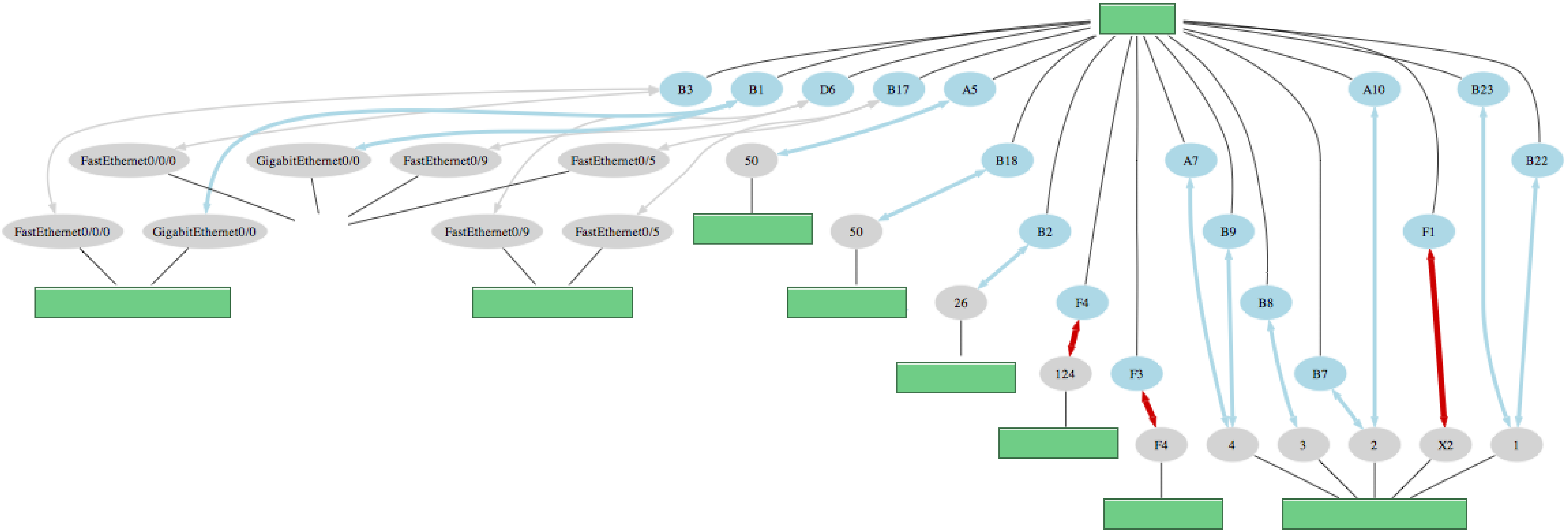
# Config example: LLDP

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

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

Main points

Configure your network equipment

Monitor your network

Control your network, react to events

Troubleshoot your network

# Learn the basics

Before running in production, and when troubleshooting

Ping traceroute - you know these, but remember that Unix traceroute can do both ICMP and 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

> *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/`

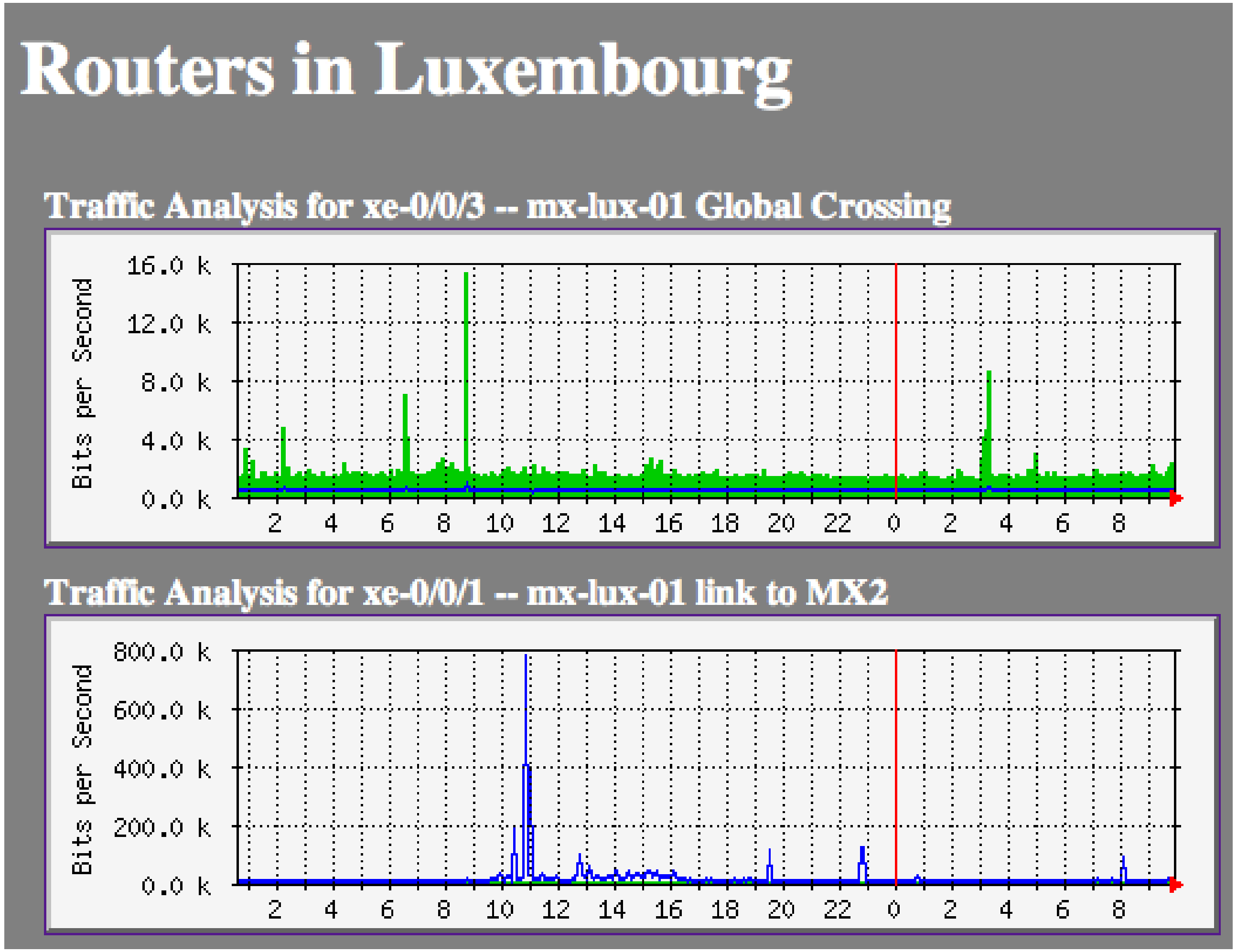
Smokeping Network Latency measurements - network quality

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

NFsen Netflow monitoring - turn on at selected routers/switches

Manual tools, my traceroute, Nping

# MRTG SNMP monitoring made easy



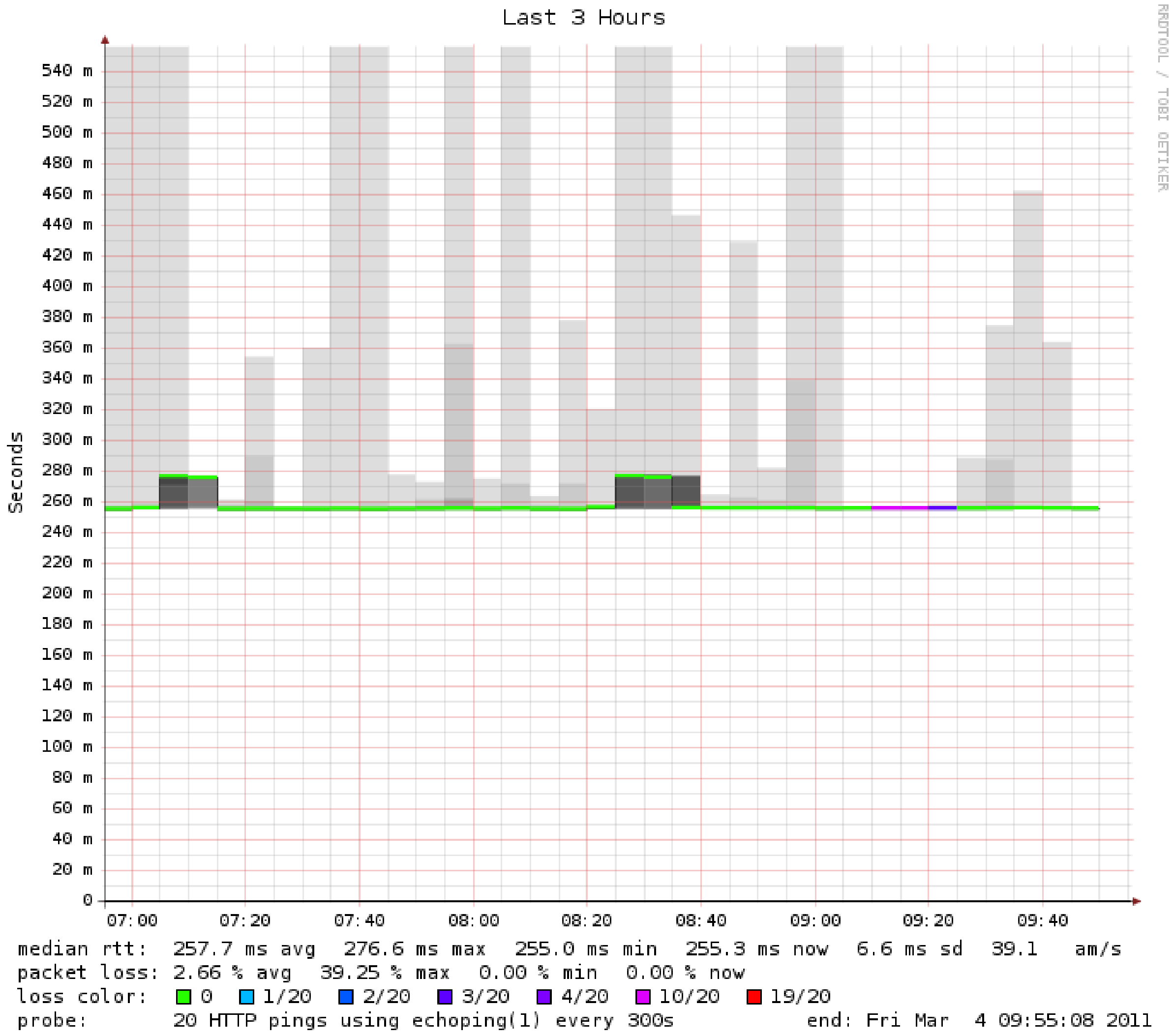
# Routers in Luxembourg

## Traffic Analysis for xe-0/0/3 -- mx-lux-01 Global Crossing

## Traffic Analysis for xe-0/0/1 -- mx-lux-01 link to MX2

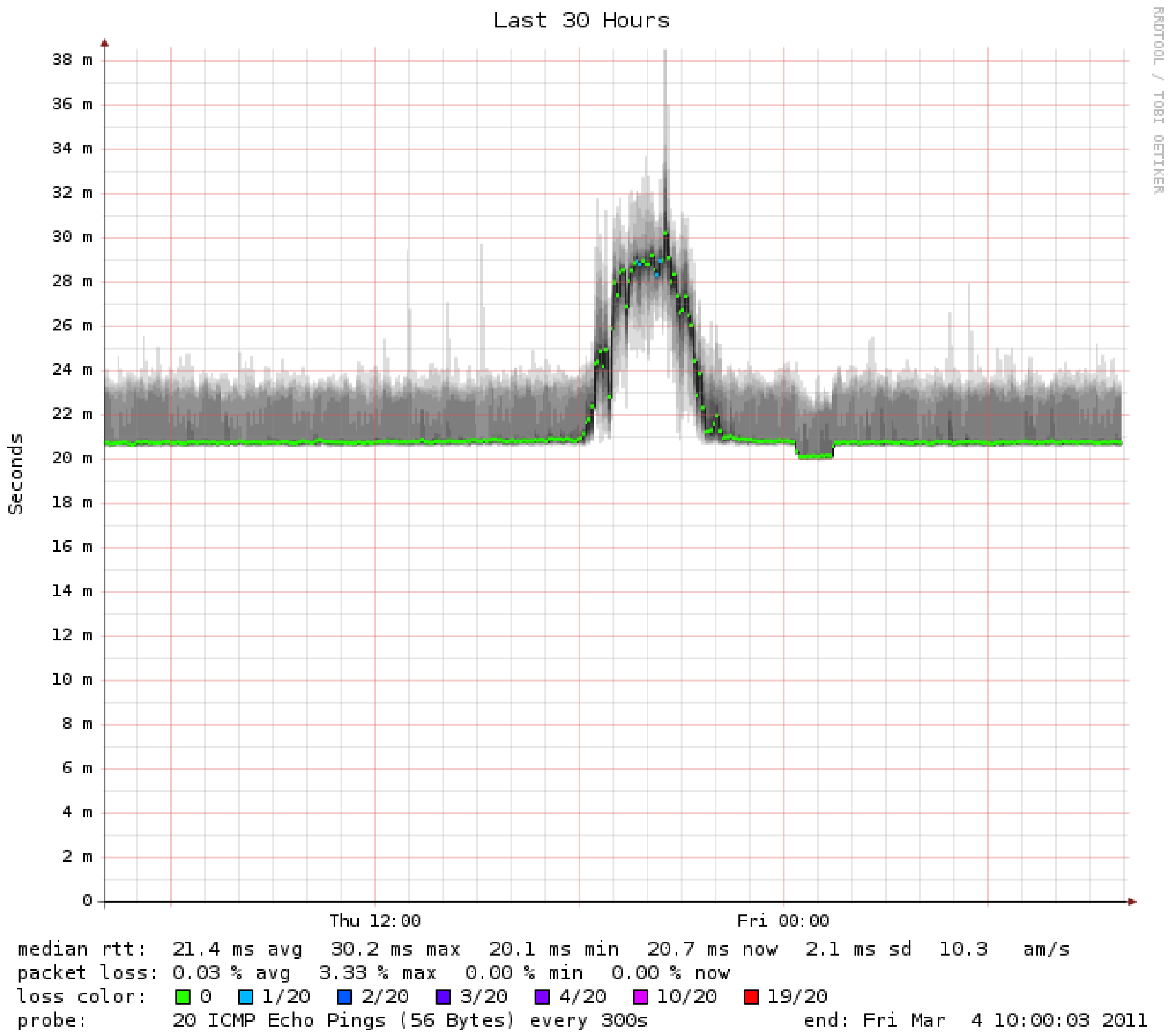
Run configmaker, indexmaker - almost done

# Smokeping packet loss



```
median rtt:   257.7 ms avg   276.6 ms max   255.0 ms min   255.3 ms now   6.6 ms sd   39.1    am/s
packet loss:  2.66 % avg   39.25 % max   0.00 % min   0.00 % now
loss color:   🟩 0   🟦 1/20   🟦 2/20   🟪 3/20   🟪 4/20   🟪 10/20   🟥 19/20
probe:        20 HTTP pings using echoping(1) every 300s          end: Fri Mar  4 09:55:08 2011
```

# Smokeping latency changed



```
median rtt:  21.4 ms avg  30.2 ms max  20.1 ms min  20.7 ms now  2.1 ms sd  10.3   am/s
packet loss: 0.03 % avg  3.33 % max  0.00 % min  0.00 % 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: Fri Mar  4 10:00:03 2011
```

# Netflow

Netflow is getting more important, more data shares the links

Accounting is important

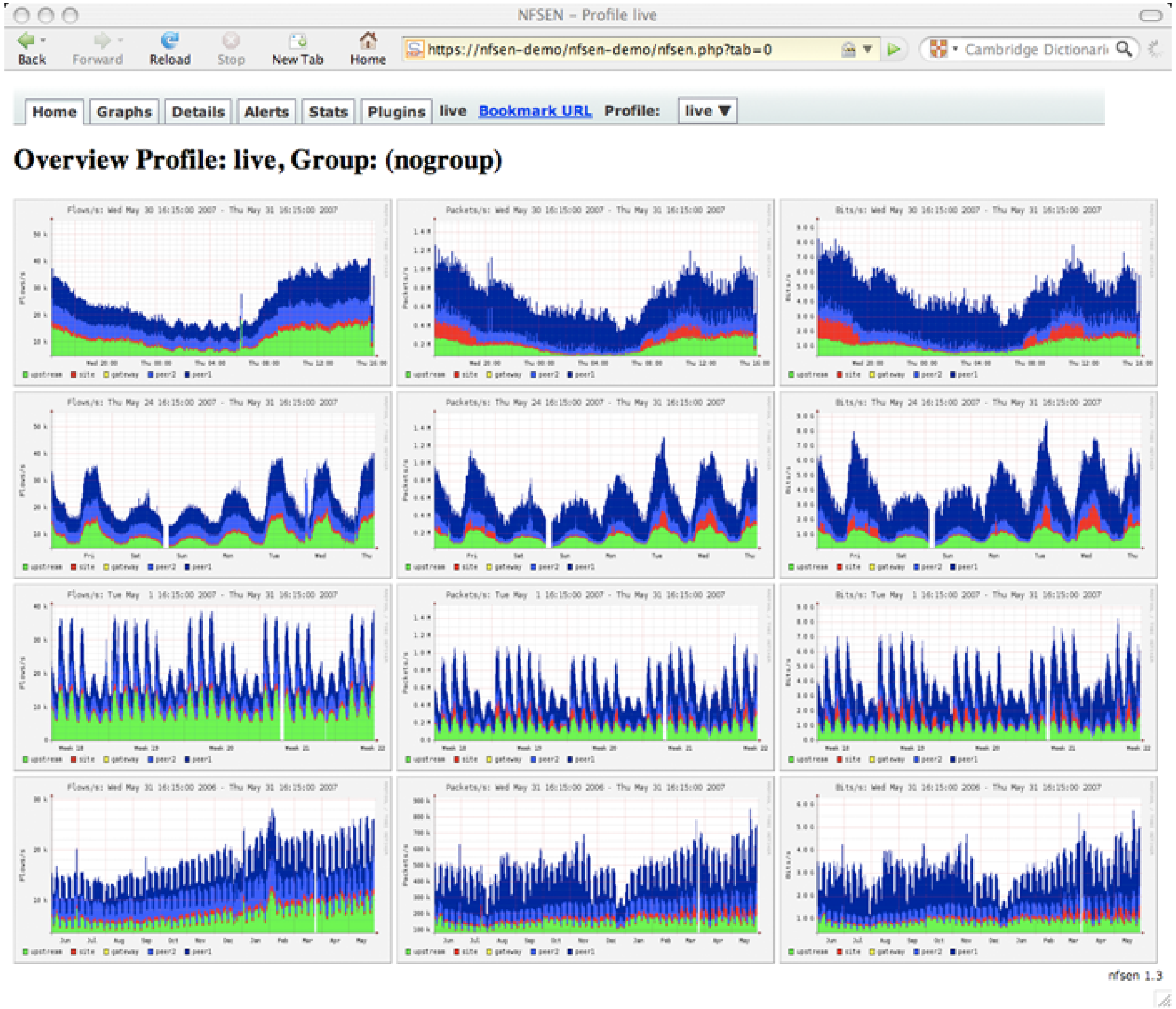
Detecting DoS/DDoS and error is essential

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


NFSEN – Profile live
Back
Forward
Reload
Stop
New Tab
Home
https://nfsen-demo/nfsen-demo/nfsen.php?tab=0
Cambridge Dictionari
Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live ▼
Flows/s: Wed May 30 16:15:00 2007 - Thu May 31 16:15:00 2007
Packets/s: Wed May 30 16:15:00 2007 - Thu May 31 16:15:00 2007
Bits/s: Wed May 30 16:15:00 2007 - Thu May 31 16:15:00 2007
Flows/s: Thu May 24 16:15:00 2007 - Thu May 31 16:15:00 2007
Packets/s: Thu May 24 16:15:00 2007 - Thu May 31 16:15:00 2007
Bits/s: Thu May 24 16:15:00 2007 - Thu May 31 16:15:00 2007
Flows/s: Tue May 1 16:15:00 2007 - Thu May 31 16:15:00 2007
Packets/s: Tue May 1 16:15:00 2007 - Thu May 31 16:15:00 2007
Bits/s: Tue May 1 16:15:00 2007 - Thu May 31 16:15:00 2007
Flows/s: Wed May 31 16:15:00 2006 - Thu May 31 16:15:00 2007
Packets/s: Wed May 31 16:15:00 2006 - Thu May 31 16:15:00 2007
Bits/s: Wed May 31 16:15:00 2006 - Thu May 31 16:15:00 2007
Flows/s
Packets/s
Bits/s
🟩 upstream 🟥 site 🟨 gateway 🟦 peer2 🟦 peer1
nfsen 1.3

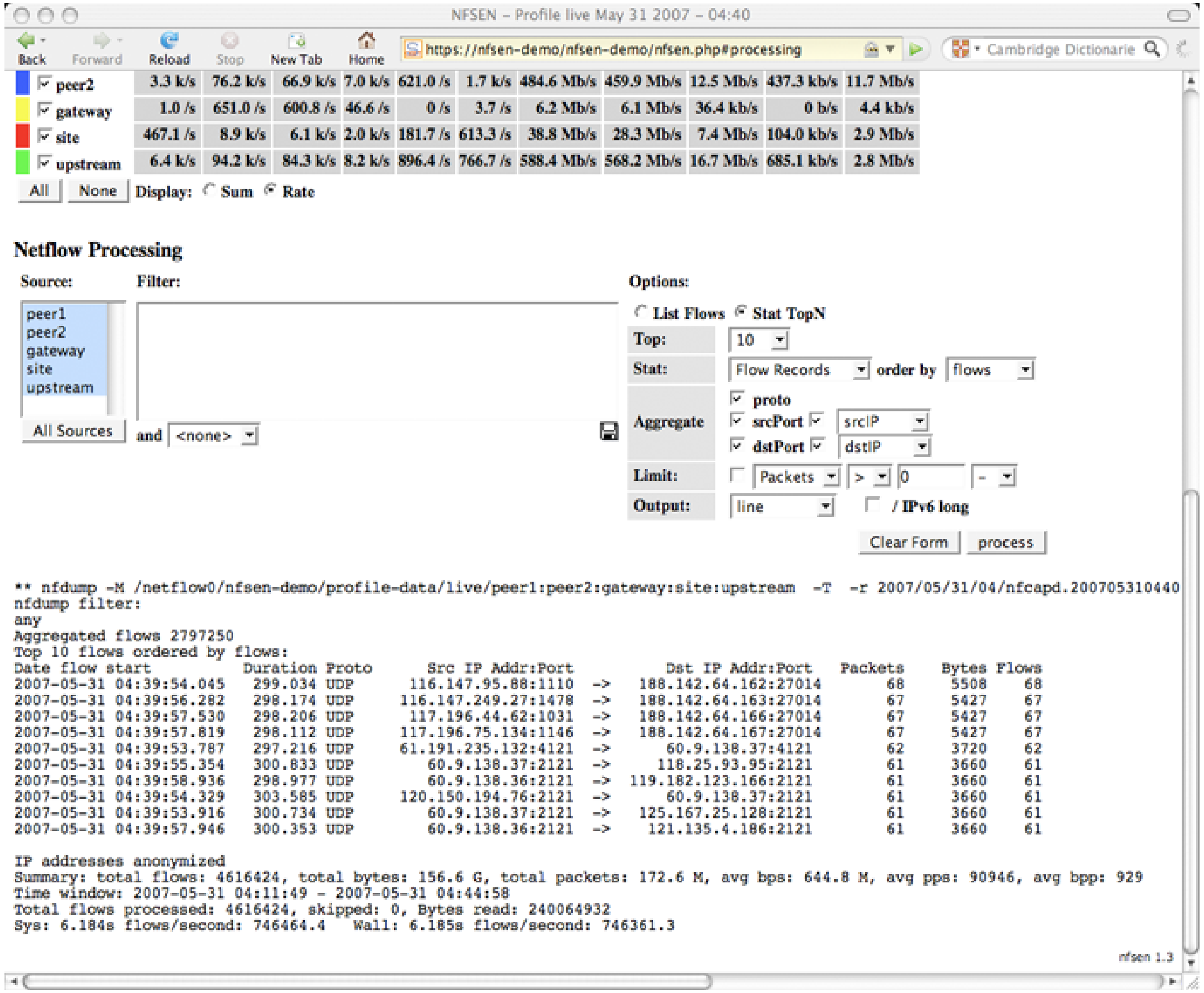
**Overview Profile: live, Group: (nogroup)**

# Netflow - nfdump

```
nfdump -R /.../2010/10/27/nfcapd.201010271200:nfcapd.201010271300 -o extended
-s record/bytes -s record/bytes -A srcip 'dst ip 91.102.88.xxx'
Aggregated flows 6
Top 10 flows ordered by bytes:
Date flow start      Duration Proto  Src IP Addr:Port       Dst IP Addr:Port  Packets
Bytes      pps      bps    Bpp Flows
2010-10-27 12:13:05.135    0.692 TCP 94.191.xxx.137:52492 -> 91.102.88.xxx:80  0     2000
953000 2890   11.0 M    476     1
2010-10-27 12:06:36.591 3055.298 TCP 212.242.xxx.112:24914 -> 91.102.88.xxx:80 0     5000
230000    1      602     46     5
2010-10-27 12:14:41.381  482.014 TCP 67.228.xxx.159:46479 -> 91.102.88.xxx:80  0     3000
 156000    6     2589     52     3
2010-10-27 12:26:02.113    0.000 TCP 94.189.xxx.255:59080 -> 91.102.88.xxx:80 136    1000
 52000    0        0     52     1
2010-10-27 12:50:02.608    0.000 TCP 66.249.xxx.176:35555 -> 91.102.88.xxx:80  0     1000
 52000    0        0     52     1
2010-10-27 12:22:09.706    0.000 TCP 212.10.xxx.190:61182 -> 91.102.88.xxx:80  0     1000
 46000    0        0     46     1

Summary: total flows: 12, total bytes: 1.5 M, total packets: 13000, avg bps: 3898,
avg pps: 4, avg bpp: 114
Time window: 2010-10-27 12:06:36 - 2010-10-27 12:57:31
Total flows processed: 129732, Blocks skipped: 0, Bytes read: 6746428
Sys: 0.012s flows/second: 9981688.1  Wall: 0.009s flows/second: 13389617.1
```

# Netflow Processing from the web interface


NFSEN – Profile live May 31 2007 – 04:40
Back
Forward
Reload
Stop
New Tab
Home
https://nfsen-demo/nfsen-demo/nfsen.php#processing
Cambridge Dictionarie

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 🟦 ☑ peer2 | 3.3 k/s | 76.2 k/s | 66.9 k/s | 7.0 k/s | 621.0 /s | 1.7 k/s | 484.6 Mb/s | 459.9 Mb/s | 12.5 Mb/s | 437.3 kb/s | 11.7 Mb/s |
| 🟨 ☑ gateway | 1.0 /s | 651.0 /s | 600.8 /s | 46.6 /s | 0 /s | 3.7 /s | 6.2 Mb/s | 6.1 Mb/s | 36.4 kb/s | 0 b/s | 4.4 kb/s |
| 🟥 ☑ site | 467.1 /s | 8.9 k/s | 6.1 k/s | 2.0 k/s | 181.7 /s | 613.3 /s | 38.8 Mb/s | 28.3 Mb/s | 7.4 Mb/s | 104.0 kb/s | 2.9 Mb/s |
| 🟩 ☑ upstream | 6.4 k/s | 94.2 k/s | 84.3 k/s | 8.2 k/s | 896.4 /s | 766.7 /s | 588.4 Mb/s | 568.2 Mb/s | 16.7 Mb/s | 685.1 kb/s | 2.8 Mb/s |

All | None | Display: ○ Sum ● Rate

**Netflow Processing**

**Source:** peer1, peer2, gateway, site, upstream | All Sources

**Filter:** and <none>

**Options:**

○ List Flows ● Stat TopN

**Top:** 10

**Stat:** Flow Records order by flows

**Aggregate** ☑ proto ☑ srcPort ☑ srcIP ☑ dstPort ☑ dstIP

**Limit:** □ Packets > 0 -

**Output:** line □ / IPv6 long

Clear Form | process

```
** nfdump -M /netflow0/nfsen-demo/profile-data/live/peer1:peer2:gateway:site:upstream  -T  -r 2007/05/31/04/nfcapd.200705310440
nfdump filter:
any
Aggregated flows 2797250
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2007-05-31 04:39:54.045   299.034 UDP     116.147.95.88:1110  ->   188.142.64.162:27014        68     5508    68
2007-05-31 04:39:56.282   298.174 UDP    116.147.249.27:1478  ->   188.142.64.163:27014        67     5427    67
2007-05-31 04:39:57.530   298.206 UDP     117.196.44.62:1031  ->   188.142.64.166:27014        67     5427    67
2007-05-31 04:39:57.819   298.112 UDP    117.196.75.134:1146  ->   188.142.64.167:27014        67     5427    67
2007-05-31 04:39:53.787   297.216 UDP    61.191.235.132:4121  ->      60.9.138.37:4121         62     3720    62
2007-05-31 04:39:55.354   300.833 UDP       60.9.138.37:2121  ->     118.25.93.95:2121         61     3660    61
2007-05-31 04:39:58.936   298.977 UDP       60.9.138.36:2121  ->  119.182.123.166:2121         61     3660    61
2007-05-31 04:39:54.329   303.585 UDP    120.150.194.76:2121  ->      60.9.138.37:2121         61     3660    61
2007-05-31 04:39:53.916   300.734 UDP       60.9.138.37:2121  ->   125.167.25.128:2121         61     3660    61
2007-05-31 04:39:57.946   300.353 UDP       60.9.138.36:2121  ->    121.135.4.186:2121         61     3660    61

IP addresses anonymized
Summary: total flows: 4616424, total bytes: 156.6 G, total packets: 172.6 M, avg bps: 644.8 M, avg pps: 90946, avg bpp: 929
Time window: 2007-05-31 04:11:49 - 2007-05-31 04:44:58
Total flows processed: 4616424, skipped: 0, Bytes read: 240064932
Sys: 6.184s flows/second: 746464.4   Wall: 6.185s flows/second: 746361.3
```

nfsen 1.3

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

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

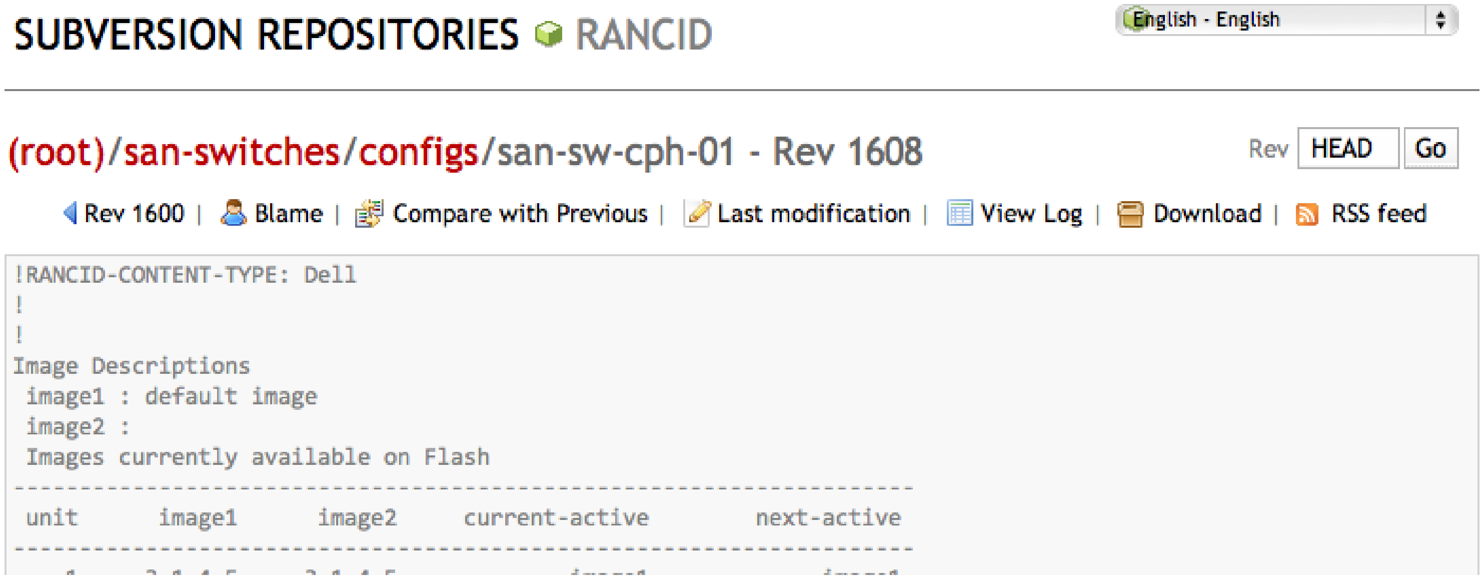
Expect, script etc. great for installing devices with common settings
`http://expect.sourceforge.net/` the expect home page

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 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

*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

```
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?

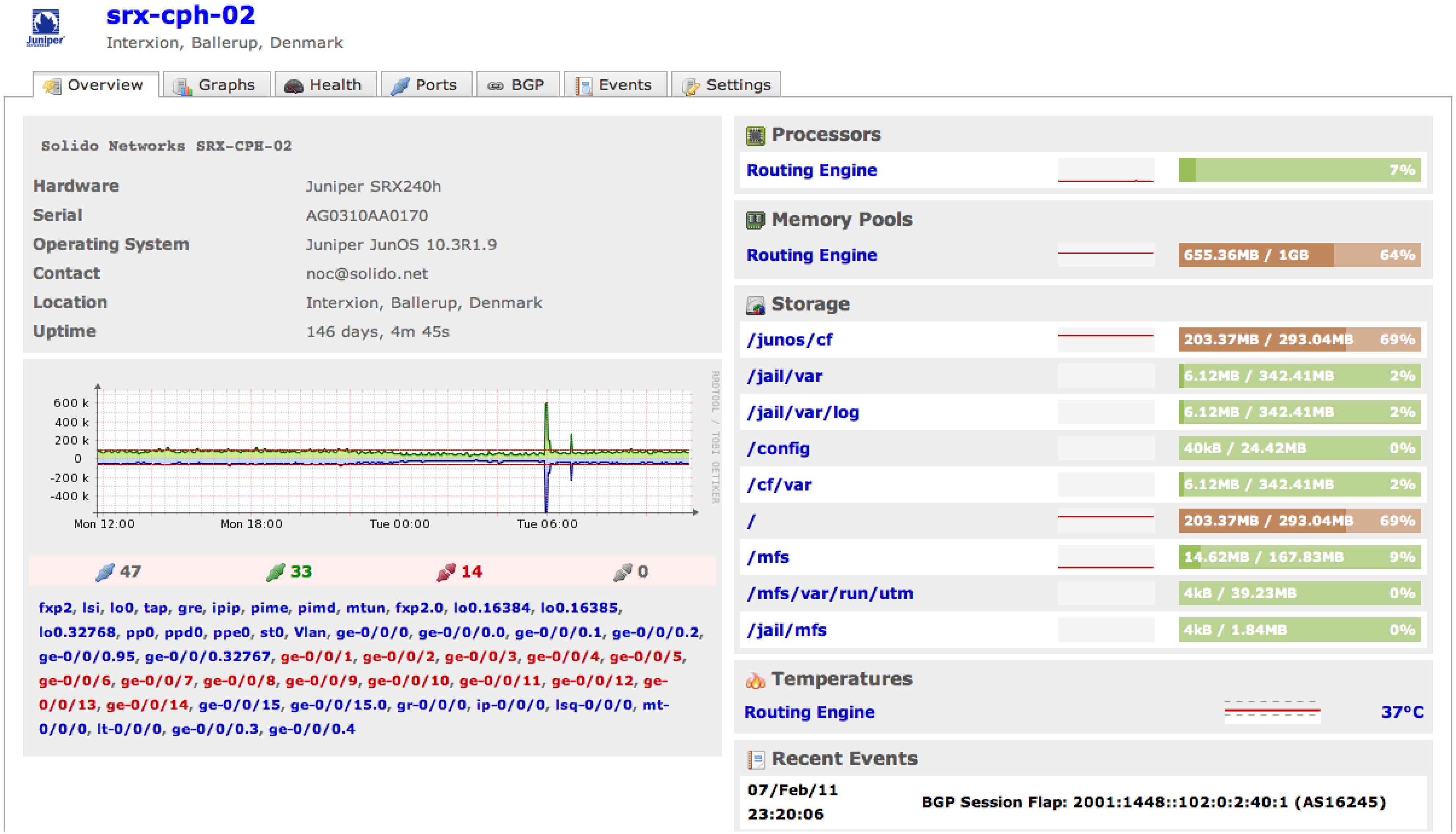
```
[root@wiseguy observium]# ./addhost.php
Add Host Tool
Usage: ./addhost.php <hostname> [community] [v1|v2c] [port]
```

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



## srx-cph-02

Interxion, Ballerup, Denmark

Solido Networks SRX-CPH-02

| | |
|---|---|
| **Hardware** | Juniper SRX240h |
| **Serial** | AG0310AA0170 |
| **Operating System** | Juniper JunOS 10.3R1.9 |
| **Contact** | noc@solido.net |
| **Location** | Interxion, Ballerup, Denmark |
| **Uptime** | 146 days, 4m 45s |

47 33 14 0

fxp2, lsi, lo0, tap, gre, ipip, pime, pimd, mtun, fxp2.0, lo0.16384, lo0.16385, lo0.32768, pp0, ppd0, ppe0, st0, Vlan, ge-0/0/0, ge-0/0/0.0, ge-0/0/0.1, ge-0/0/0.2, ge-0/0/0.95, ge-0/0/0.32767, ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/4, ge-0/0/5, ge-0/0/6, ge-0/0/7, ge-0/0/8, ge-0/0/9, ge-0/0/10, ge-0/0/11, ge-0/0/12, ge-0/0/13, ge-0/0/14, ge-0/0/15, ge-0/0/15.0, gr-0/0/0, ip-0/0/0, lsq-0/0/0, mt-0/0/0, lt-0/0/0, ge-0/0/0.3, ge-0/0/0.4

### Processors

| | | |
|---|---|---|
| Routing Engine | | 7% |

### Memory Pools

| | | |
|---|---|---|
| Routing Engine | 655.36MB / 1GB | 64% |

### Storage

| | | |
|---|---|---|
| /junos/cf | 203.37MB / 293.04MB | 69% |
| /jail/var | 6.12MB / 342.41MB | 2% |
| /jail/var/log | 6.12MB / 342.41MB | 2% |
| /config | 40kB / 24.42MB | 0% |
| /cf/var | 6.12MB / 342.41MB | 2% |
| / | 203.37MB / 293.04MB | 69% |
| /mfs | 14.62MB / 167.83MB | 9% |
| /mfs/var/run/utm | 4kB / 39.23MB | 0% |
| /jail/mfs | 4kB / 1.84MB | 0% |

### Temperatures

| | |
|---|---|
| Routing Engine | 37°C |

### Recent Events

| | |
|---|---|
| 07/Feb/11 23:20:06 | BGP Session Flap: 2001:1448::102:0:2:40:1 (AS16245) |

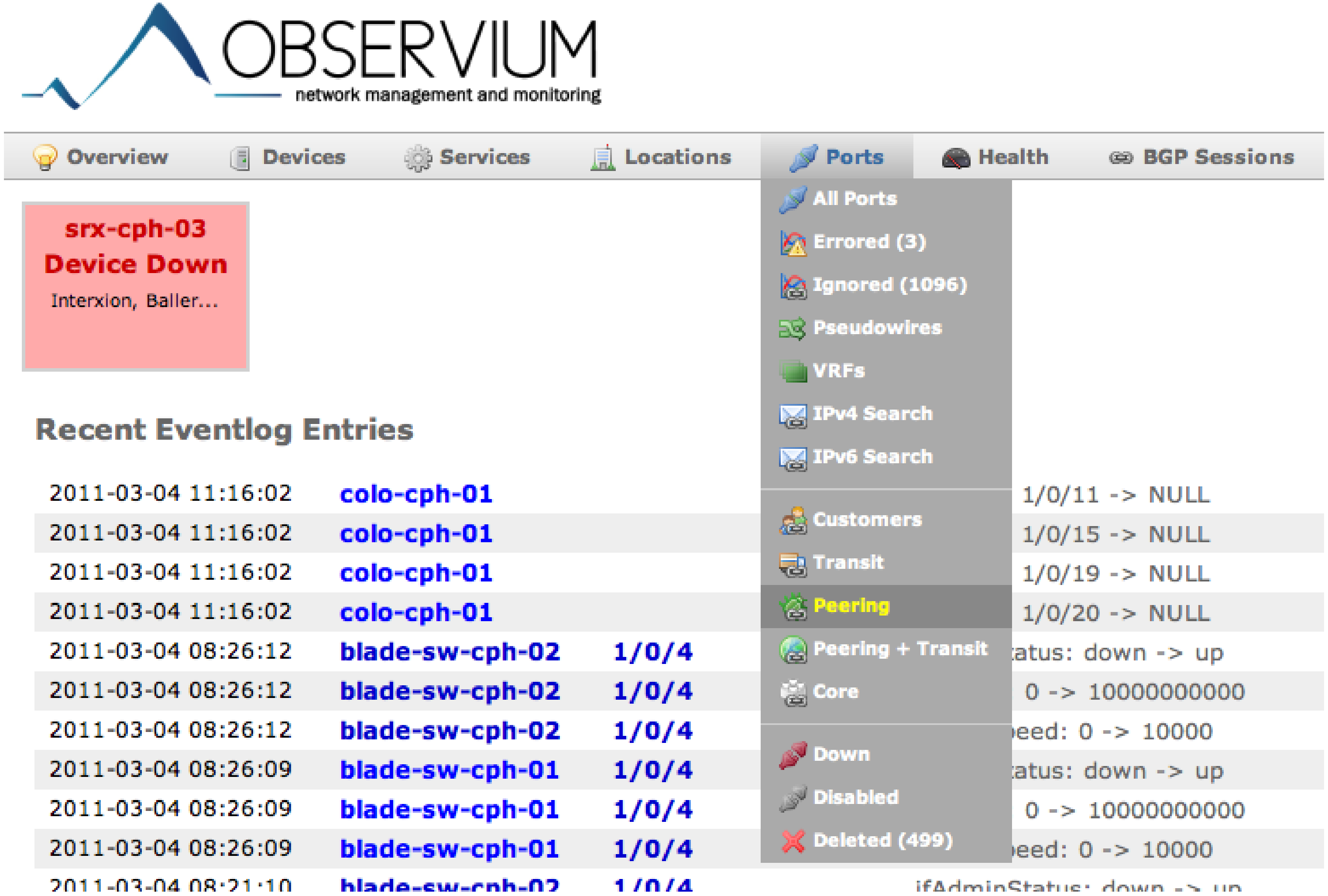
More useful information than default vendor interface! (flash)

# 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";
```

# Overview ports

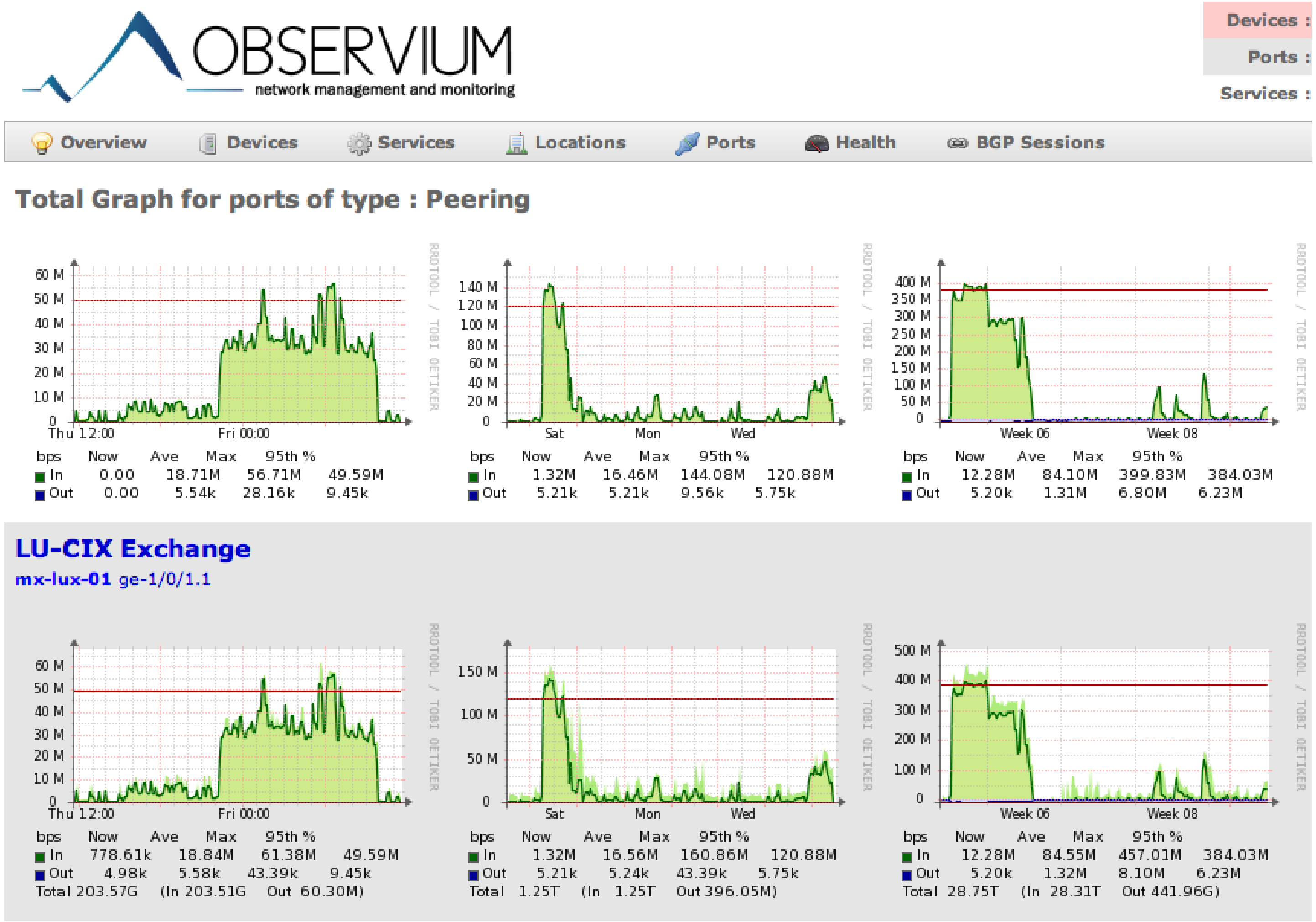


**srx-cph-03**
**Device Down**
Interxion, Baller...

## Recent Eventlog Entries

| | | | |
|---|---|---|---|
| 2011-03-04 11:16:02 | colo-cph-01 | | 1/0/11 -> NULL |
| 2011-03-04 11:16:02 | colo-cph-01 | | 1/0/15 -> NULL |
| 2011-03-04 11:16:02 | colo-cph-01 | | 1/0/19 -> NULL |
| 2011-03-04 11:16:02 | colo-cph-01 | | 1/0/20 -> NULL |
| 2011-03-04 08:26:12 | blade-sw-cph-02 | 1/0/4 | atus: down -> up |
| 2011-03-04 08:26:12 | blade-sw-cph-02 | 1/0/4 | 0 -> 10000000000 |
| 2011-03-04 08:26:12 | blade-sw-cph-02 | 1/0/4 | eed: 0 -> 10000 |
| 2011-03-04 08:26:09 | blade-sw-cph-01 | 1/0/4 | atus: down -> up |
| 2011-03-04 08:26:09 | blade-sw-cph-01 | 1/0/4 | 0 -> 10000000000 |
| 2011-03-04 08:26:09 | blade-sw-cph-01 | 1/0/4 | eed: 0 -> 10000 |
| 2011-03-04 08:21:10 | blade-sw-cph-02 | 1/0/4 | ifAdminStatus: down -> up |

# Overview peering ports



Total Graph for ports of type : Peering

```
bps   Now     Ave      Max      95th %
In    0.00    18.71M   56.71M   49.59M
Out   0.00    5.54k    28.16k   9.45k
```

```
bps   Now     Ave      Max      95th %
In    1.32M   16.46M   144.08M  120.88M
Out   5.21k   5.21k    9.56k    5.75k
```

```
bps   Now     Ave      Max      95th %
In    12.28M  84.10M   399.83M  384.03M
Out   5.20k   1.31M    6.80M    6.23M
```

LU-CIX Exchange

mx-lux-01 ge-1/0/1.1

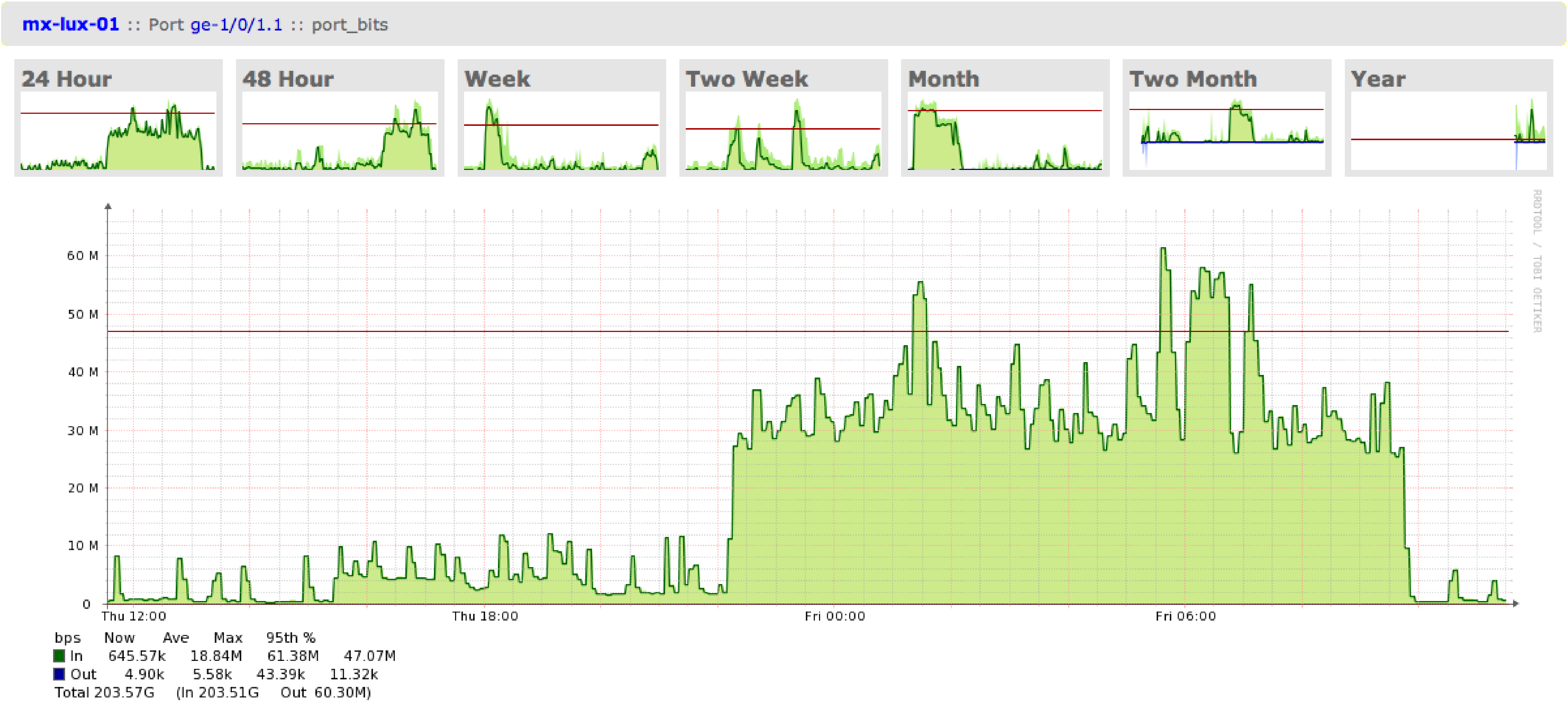
```
bps   Now      Ave      Max      95th %
In    778.61k  18.84M   61.38M   49.59M
Out   4.98k    5.58k    43.39k   9.45k
Total 203.57G  (In 203.51G   Out  60.30M)
```

```
bps   Now     Ave      Max      95th %
In    1.32M   16.56M   160.86M  120.88M
Out   5.21k   5.24k    43.39k   5.75k
Total  1.25T   (In  1.25T   Out 396.05M)
```

```
bps   Now     Ave      Max      95th %
In    12.28M  84.55M   457.01M  384.03M
Out   5.20k   1.32M    8.10M    6.23M
Total  28.75T  (In  28.31T   Out 441.96G)
```

(does not show all peerings we have)

# Overview ports

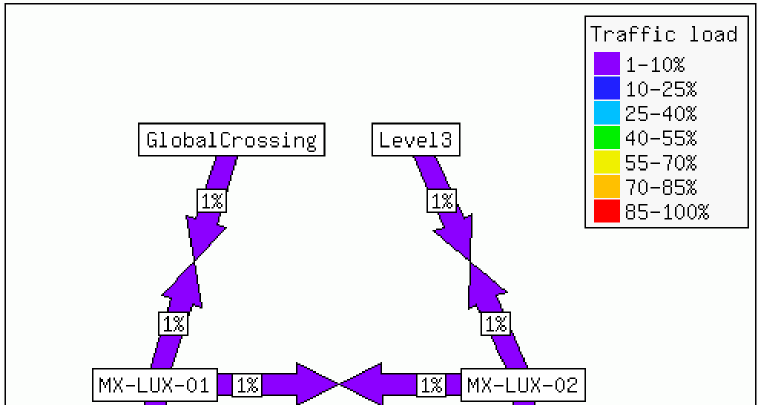


mx-lux-01 :: Port ge-1/0/1.1 :: port_bits

```
bps     Now       Ave       Max      95th %
🟩 In    645.57k    18.84M    61.38M    47.07M
🟦 Out     4.90k     5.58k    43.39k    11.32k
Total 203.57G    (In 203.51G    Out  60.30M)
```

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 important

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

# Embrace, extend and proliferate

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

# Checklist

Get tools, start downloading BT4 now

Learn Unix

Configure devices, Hint: expect and/or RANCID clogin

# Web sites

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

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

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

Rancid, syslog, grep, Perl, PHP, NetFlow, and proprietary scripting.

# Disclaimer: commercial tools

# Questions?

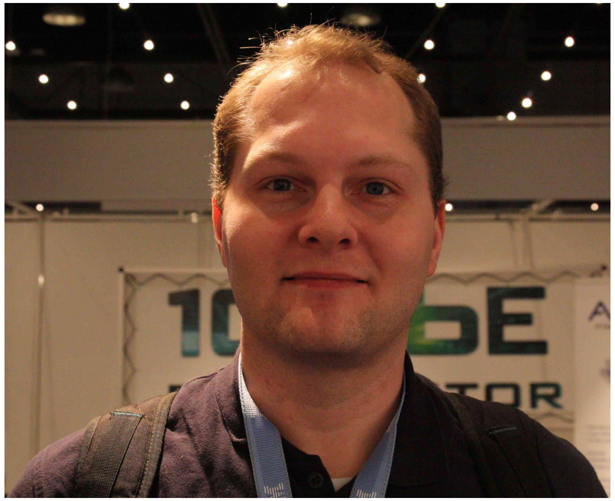
Henrik Lund Kramshøj
hlk@solidonetworks.com

`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