# ABCs of Network Monitoring

## Automated Intelligence

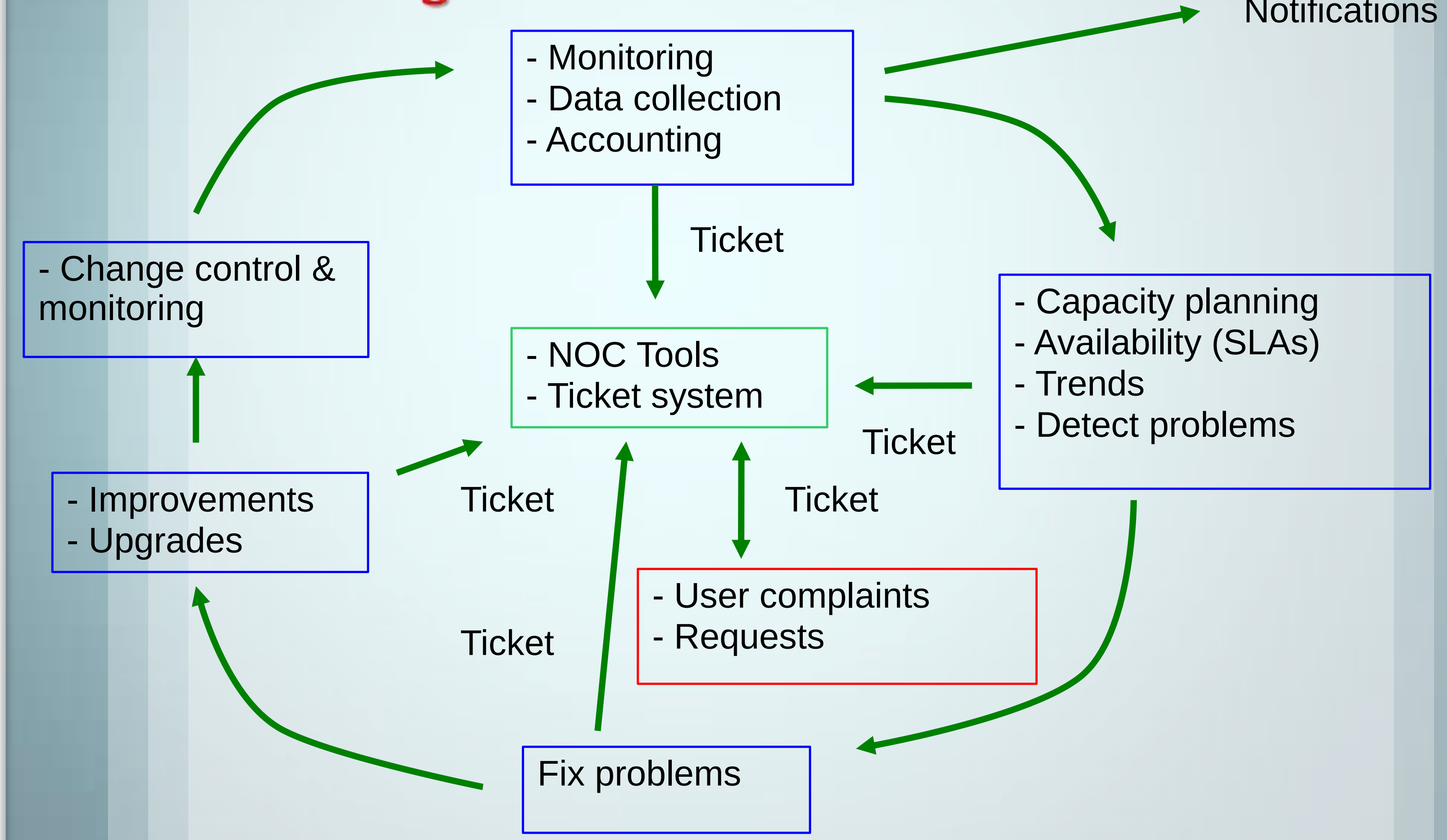
**GZ Kabir**
BDCOM ONLINE LTD.

# Agenda

- □ Network Monitoring
  - Perspectives
  - Components
  - Tools
  - Demonstration

# Big picture – First View

- How it all fits together



Notifications

- Monitoring
- Data collection
- Accounting

Ticket

- Change control & monitoring

- NOC Tools
- Ticket system

- Capacity planning
- Availability (SLAs)
- Trends
- Detect problems

Ticket

- Improvements
- Upgrades

Ticket

Ticket

- User complaints
- Requests

Ticket

Fix problems

# Perspectives

□ **Operation:**

keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

□ **Administration:**

deals with keeping track of resources in the network and how they are assigned.

□ **Maintenance:**

concerned with performing repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run "better".

□ **Provisioning:**

is concerned with configuring resources in the network to support a given service.

# So …

Network Management is the use of a system that constantly monitors a computer network for slow or failing systems and that notifies the network administrator in case of outages via email, SMS or other alert Mechanisms.

subset of the functions involved in network management.

# Network Mangement

- System & Service monitoring
  - Reachability, availability
- Resource measurement/monitoring
  - Capacity planning, availability
- Performance monitoring (RTT, throughput)
- Stats & Accounting/Metering
- Fault Management
  - Fault detection, troubleshooting, and tracking
- Configuration/Change Management
- Coordination
- & So on ...

# Components

- □ Availability
- □ Reliability
- □ Performance
- □ Configuration Mgmt & Monitoring
- □ Network Forensic
- □ Intrusion Detection …
- □ ….
- □ …..
- □ Coordination

# Tools

- **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools
- **Monitoring tools** – tools running in the background (”daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.
- **Performance tools** – tell us how our network is handling traffic flow.

# Tools

- Active tools
  - Ping – test connectivity to a host
  - Traceroute – show path to a host
  - MTR – combination of ping + traceroute
  - SNMP collectors (polling)
- Passive tools
  - log monitoring, SNMP trap receivers
- Automated tools
  - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
  - MRTG – record and graph bandwidth usage on a switch port or network link, at regular intervals
  - So **MANY** More .....

# Log, Log, Log ….

The Bible

# Components

□ Availability

□ Reliability

□ Performance

□ Configuration Mgmt & Monitoring

□ Network Forensic

□ Intrusion Detection …

□ ….

□ …..

□ Coordination

# Tools … Availability

- Nagios
  - server and service availability monitoring
    - Can monitor pretty much anything
    - HTTP, SMTP, DNS, Disk space, CPU usage, …
    - BGP, OSPF, Switch Port, room temperature, ..
    - Easy to write new plugins (extensions)
- Zabbix, ZenOSS, Hyperic, … Many more Open Source…

- Logging capability
- Notification mechanism

# NAGIOS

- Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes
- A key measurement tool for actively monitoring availability of devices and services.
- Possibly the most used open source network monitoring software.
- Has a web interface.
  - Uses CGIs written in C for faster response and scalability.
- Can support up to thousands of devices and services.

# How Nagios Works

- Checks services
- If the service is down, checks the host
- If the host is down, checks its parent
- Find the highest-level thing that's down
- Retest it a few times (e.g. 5 or 10 times)
- If it stays down:
  - Figure out who to notify
  - Send them a message
  - Keep notifying them until it comes back up
- **It nags us!**

# Advantages of Nagios

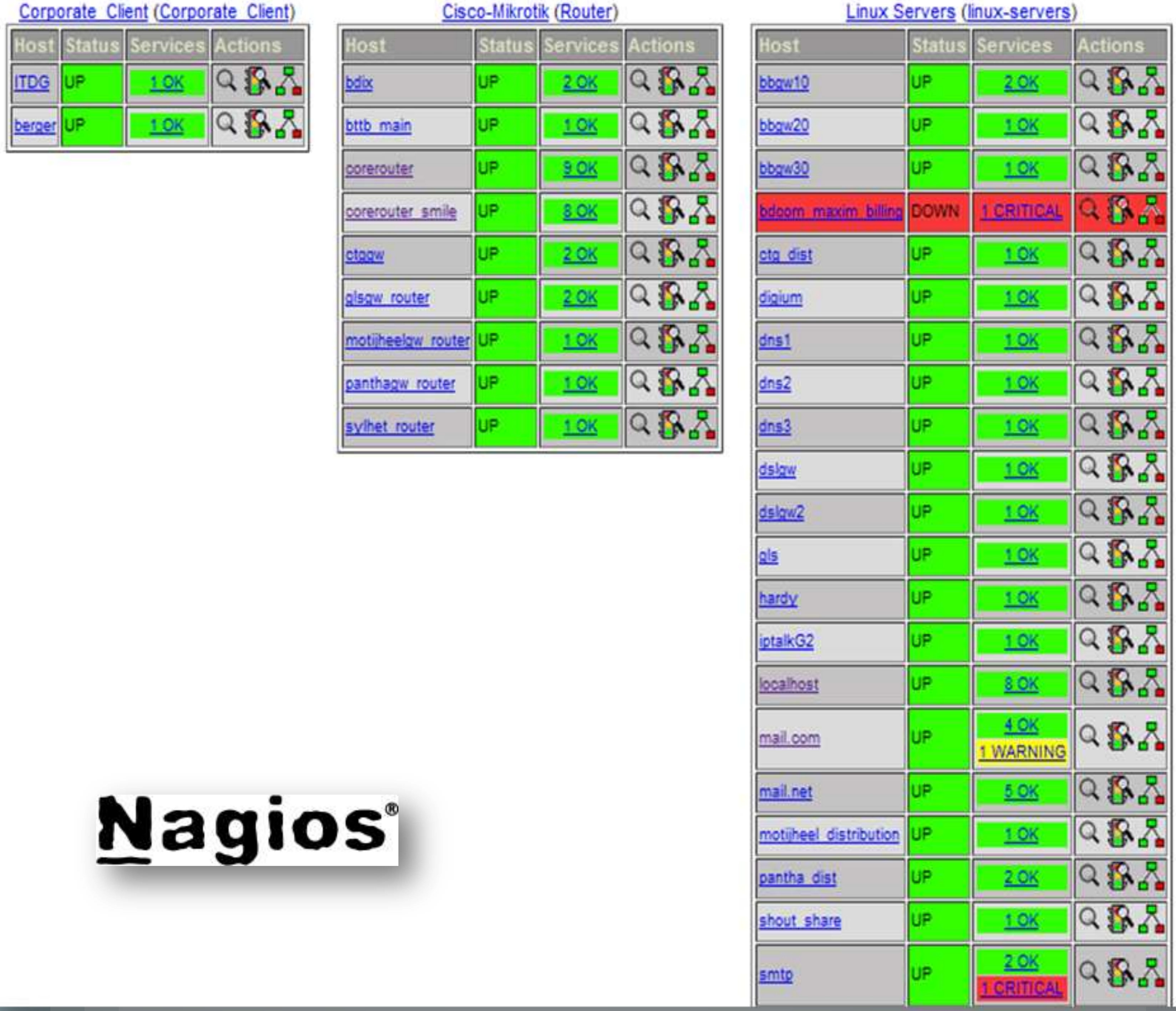
- Small, relatively easy to understand
- Lightweight and fast
- Easy to extend (write new plugins)
- Large library of agent-less monitoring plugins
- Agents for Windows and most Unixes
- Free and open source

Nagios Plugins/addons

# Nagios Exchange

- □**Addons** (537)
- □**Certified Compatible** (3)
- □**Comparisons** (8)
- □**Cool Stuff** (6)
- □**Demos** (3)
- □**Distributions** (18)
- □**Documentation** (123)
- □**Graphics and Logos** (35)
- □**Media Coverage** (5)
- □**Multimedia** (104)
- □**Patches** (20)
- □**Plugins** (2593)
- □**Seedcamp** (14)
- □**Translations** (9)
- □**Tutorials** (299)
- □**Uncategorized** (0)
- □**Utilities** (14)

# Tools …. Nagios



Corporate_Client (Corporate_Client)

| Host | Status | Services | Actions |
|---|---|---|---|
| ITDG | UP | 1 OK | 🔍 🚦 🖧 |
| berger | UP | 1 OK | 🔍 🚦 🖧 |

Cisco-Mikrotik (Router)

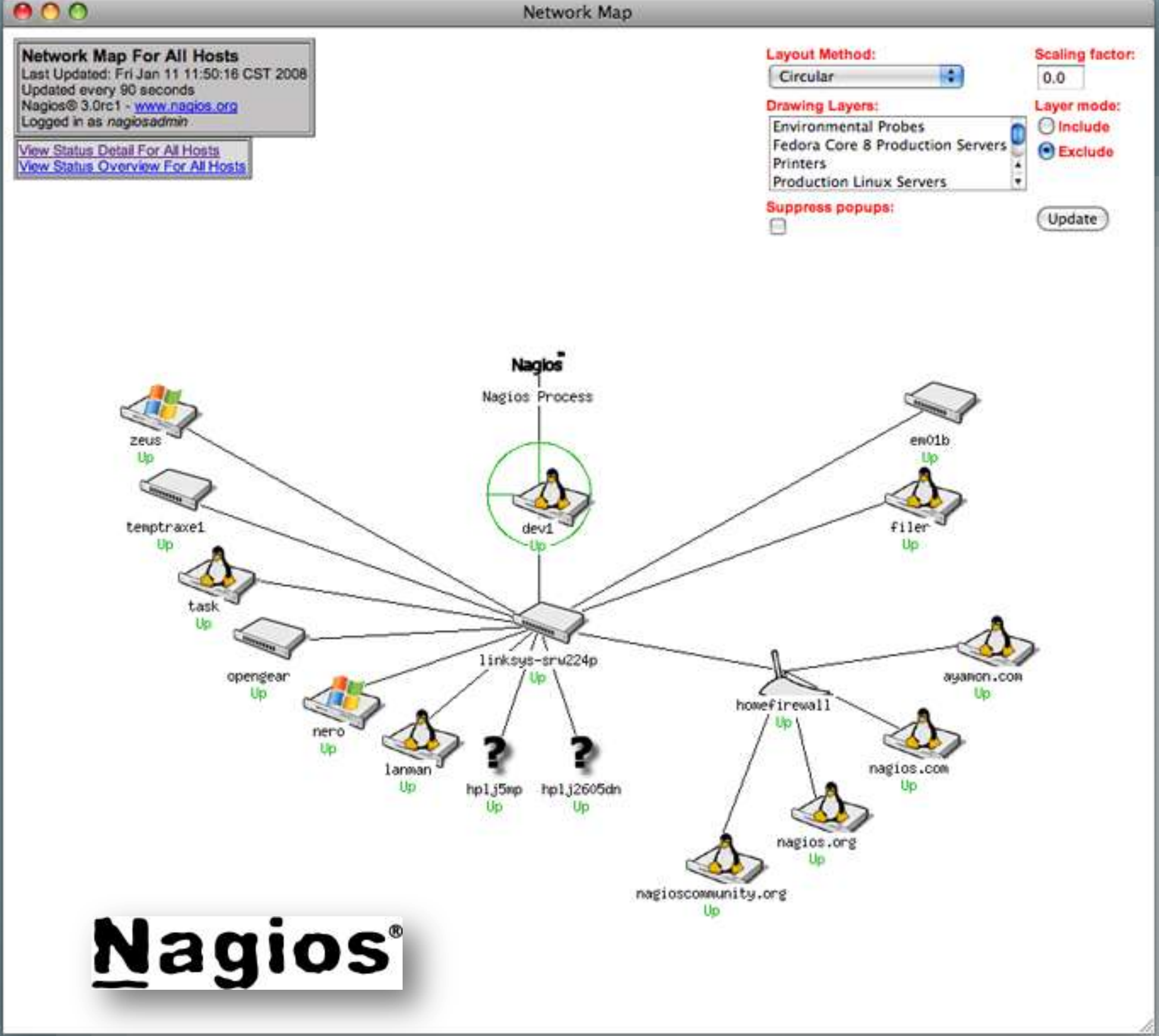
| Host | Status | Services | Actions |
|---|---|---|---|
| bdix | UP | 2 OK | 🔍 🚦 🖧 |
| bttb_main | UP | 1 OK | 🔍 🚦 🖧 |
| corerouter | UP | 9 OK | 🔍 🚦 🖧 |
| corerouter_smile | UP | 8 OK | 🔍 🚦 🖧 |
| ctggw | UP | 2 OK | 🔍 🚦 🖧 |
| glsgw_router | UP | 2 OK | 🔍 🚦 🖧 |
| motijheelgw_router | UP | 1 OK | 🔍 🚦 🖧 |
| panthagw_router | UP | 1 OK | 🔍 🚦 🖧 |
| sylhet_router | UP | 1 OK | 🔍 🚦 🖧 |

Linux Servers (linux-servers)

| Host | Status | Services | Actions |
|---|---|---|---|
| bbgw10 | UP | 2 OK | 🔍 🚦 🖧 |
| bbgw20 | UP | 1 OK | 🔍 🚦 🖧 |
| bbgw30 | UP | 1 OK | 🔍 🚦 🖧 |
| bdcom_maxim_billing | DOWN | 1 CRITICAL | 🔍 🚦 🖧 |
| ctg_dist | UP | 1 OK | 🔍 🚦 🖧 |
| digium | UP | 1 OK | 🔍 🚦 🖧 |
| dns1 | UP | 1 OK | 🔍 🚦 🖧 |
| dns2 | UP | 1 OK | 🔍 🚦 🖧 |
| dns3 | UP | 1 OK | 🔍 🚦 🖧 |
| dslgw | UP | 1 OK | 🔍 🚦 🖧 |
| dslgw2 | UP | 1 OK | 🔍 🚦 🖧 |
| gls | UP | 1 OK | 🔍 🚦 🖧 |
| hardy | UP | 1 OK | 🔍 🚦 🖧 |
| iptalkG2 | UP | 1 OK | 🔍 🚦 🖧 |
| localhost | UP | 8 OK | 🔍 🚦 🖧 |
| mail.com | UP | 4 OK<br>1 WARNING | 🔍 🚦 🖧 |
| mail.net | UP | 5 OK | 🔍 🚦 🖧 |
| motijheel_distribution | UP | 1 OK | 🔍 🚦 🖧 |
| pantha_dist | UP | 2 OK | 🔍 🚦 🖧 |
| shout_share | UP | 1 OK | 🔍 🚦 🖧 |
| smtp | UP | 2 OK<br>1 CRITICAL | 🔍 🚦 🖧 |

Nagios®

# Tools … Nagios



Network Map

**Network Map For All Hosts**
Last Updated: Fri Jan 11 11:50:16 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For All Hosts
View Status Overview For All Hosts

Layout Method: Circular

Scaling factor: 0.0

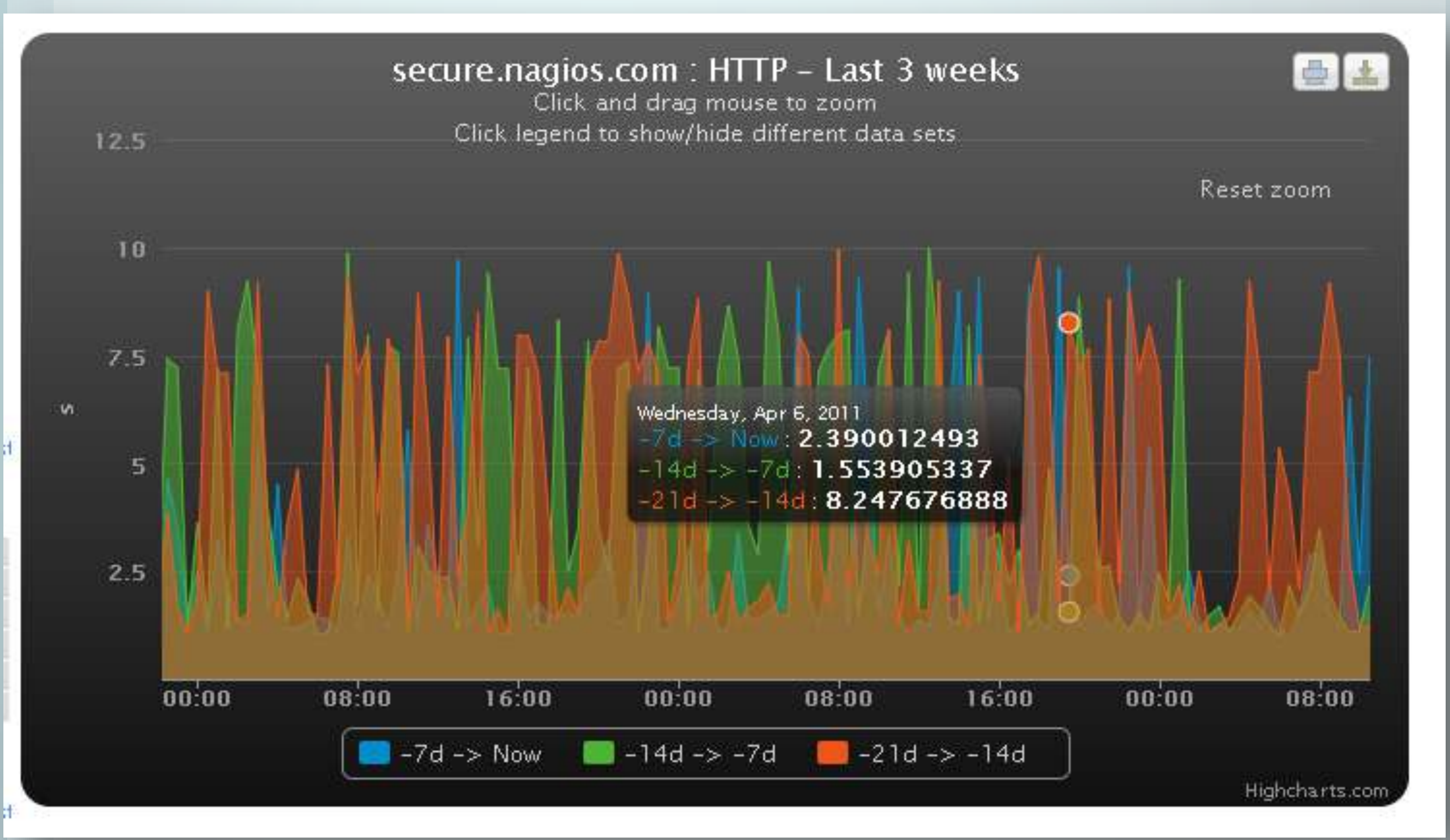
Drawing Layers:
Environmental Probes
Fedora Core 8 Production Servers
Printers
Production Linux Servers

Layer mode: ○ Include ● Exclude

Suppress popups: □

# Tools …. Nagios

Nagios®



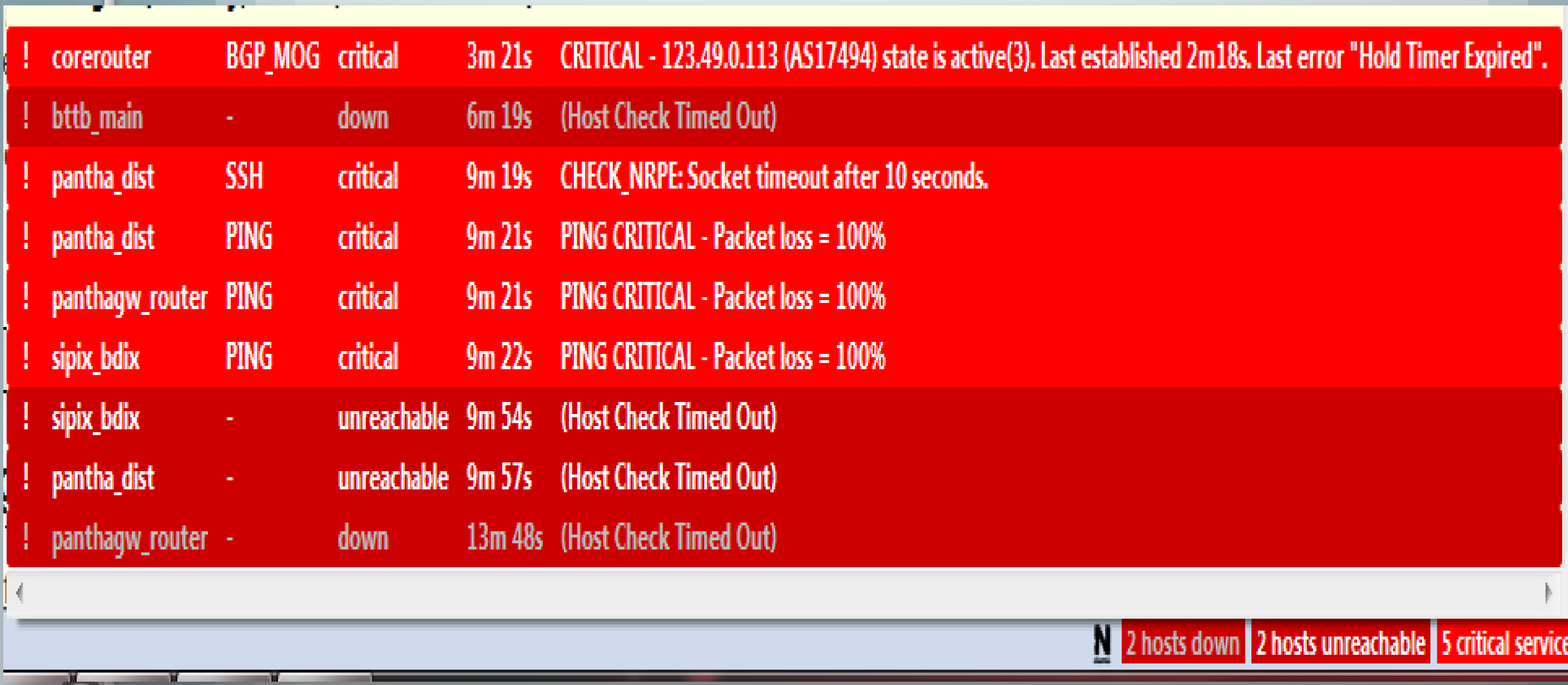
secure.nagios.com : HTTP – Last 3 weeks

Click and drag mouse to zoom

Click legend to show/hide different data sets

Wednesday, Apr 6, 2011
-7d -> Now : 2.390012493
-14d -> -7d : 1.553905337
-21d -> -14d : 8.247676888

Nagios

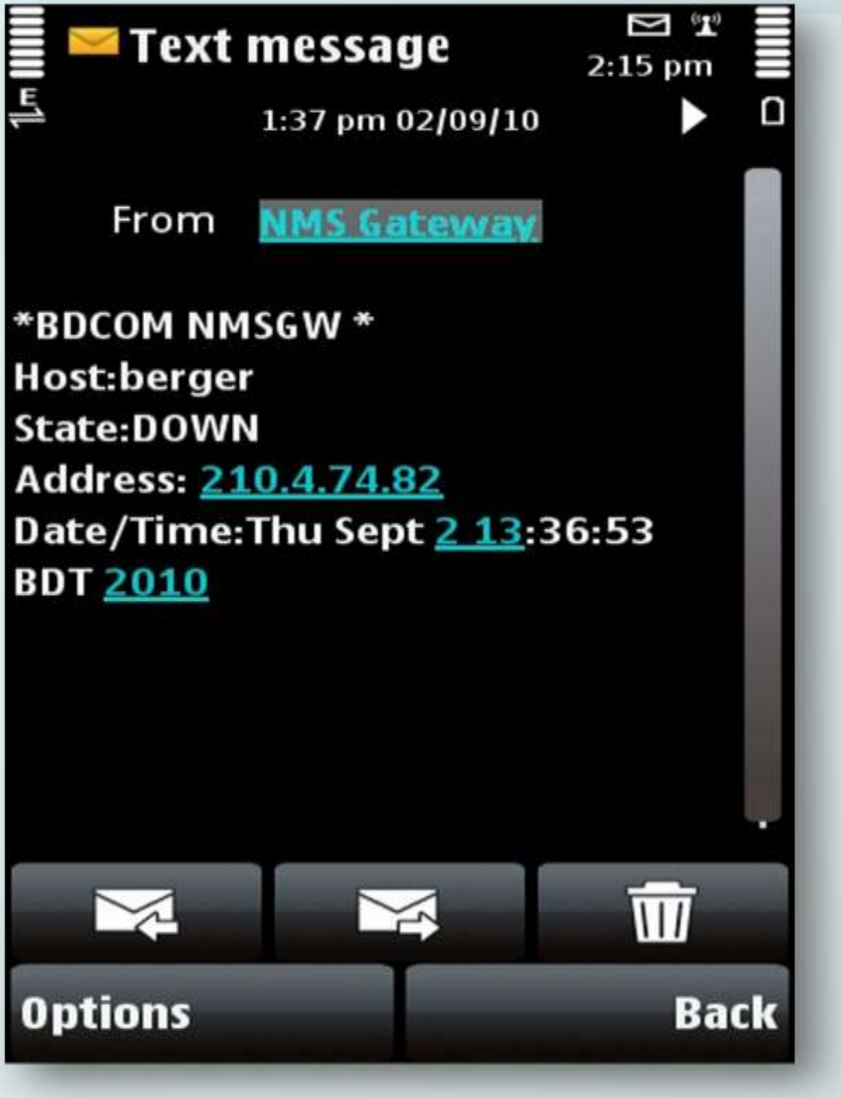


```
! corerouter      BGP_MOG  critical     3m 21s   CRITICAL - 123.49.0.113 (AS17494) state is active(3). Last established 2m18s. Last error "Hold Timer Expired".
! bttb_main       -        down         6m 19s   (Host Check Timed Out)
! pantha_dist     SSH      critical     9m 19s   CHECK_NRPE: Socket timeout after 10 seconds.
! pantha_dist     PING     critical     9m 21s   PING CRITICAL - Packet loss = 100%
! panthagw_router PING     critical     9m 21s   PING CRITICAL - Packet loss = 100%
! sipix_bdix      PING     critical     9m 22s   PING CRITICAL - Packet loss = 100%
! sipix_bdix      -        unreachable  9m 54s   (Host Check Timed Out)
! pantha_dist     -        unreachable  9m 57s   (Host Check Timed Out)
! panthagw_router -        down         13m 48s  (Host Check Timed Out)
```

Too

# Tools .... Nagios

Nagios



1:37 pm 02/09/10

From NMS Gateway

*BDCOM NMSGW *
Host:berger
State:DOWN
Address: 210.4.74.82
Date/Time:Thu Sept 2 13:36:53
BDT 2010

# Components

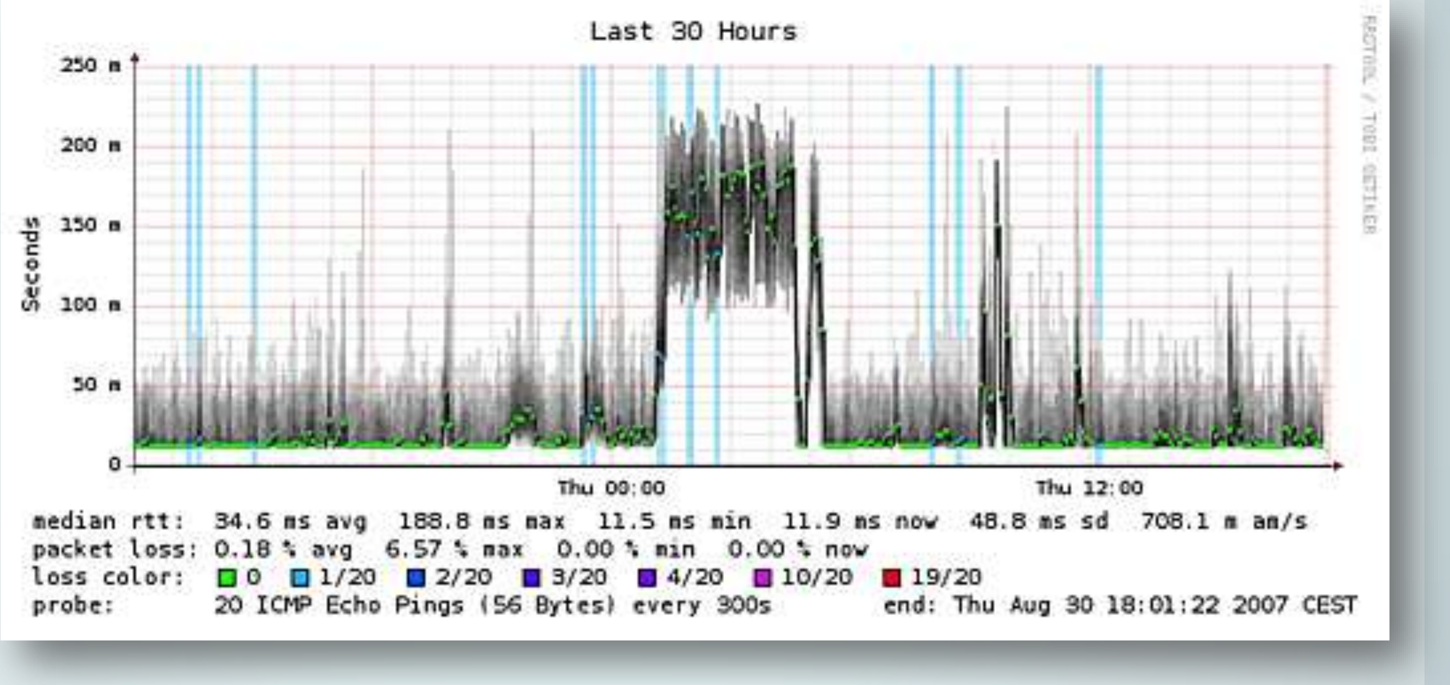
- □ Availability
- □ Reliability
- □ Performance
- □ Configuration Mgmt & Monitoring
- □ Network Forensic
- □ Intrusion Detection …
- □ ….
- □ …..
- □ Coordination

# Tools ... Reliability

- □ SmokePing
  - Keeps track of your network latency:
  - Best of breed latency visualisation.
  - Interactive graph explorer.
  - Wide range of latency measurment plugins.
  - Master/Slave System for distributed measurement.
  - Highly configurable alerting system.
  - Live Latency Charts with the most 'interesting' graphs.
  - Free and OpenSource Software written in Perl

# Tools … SmokePing

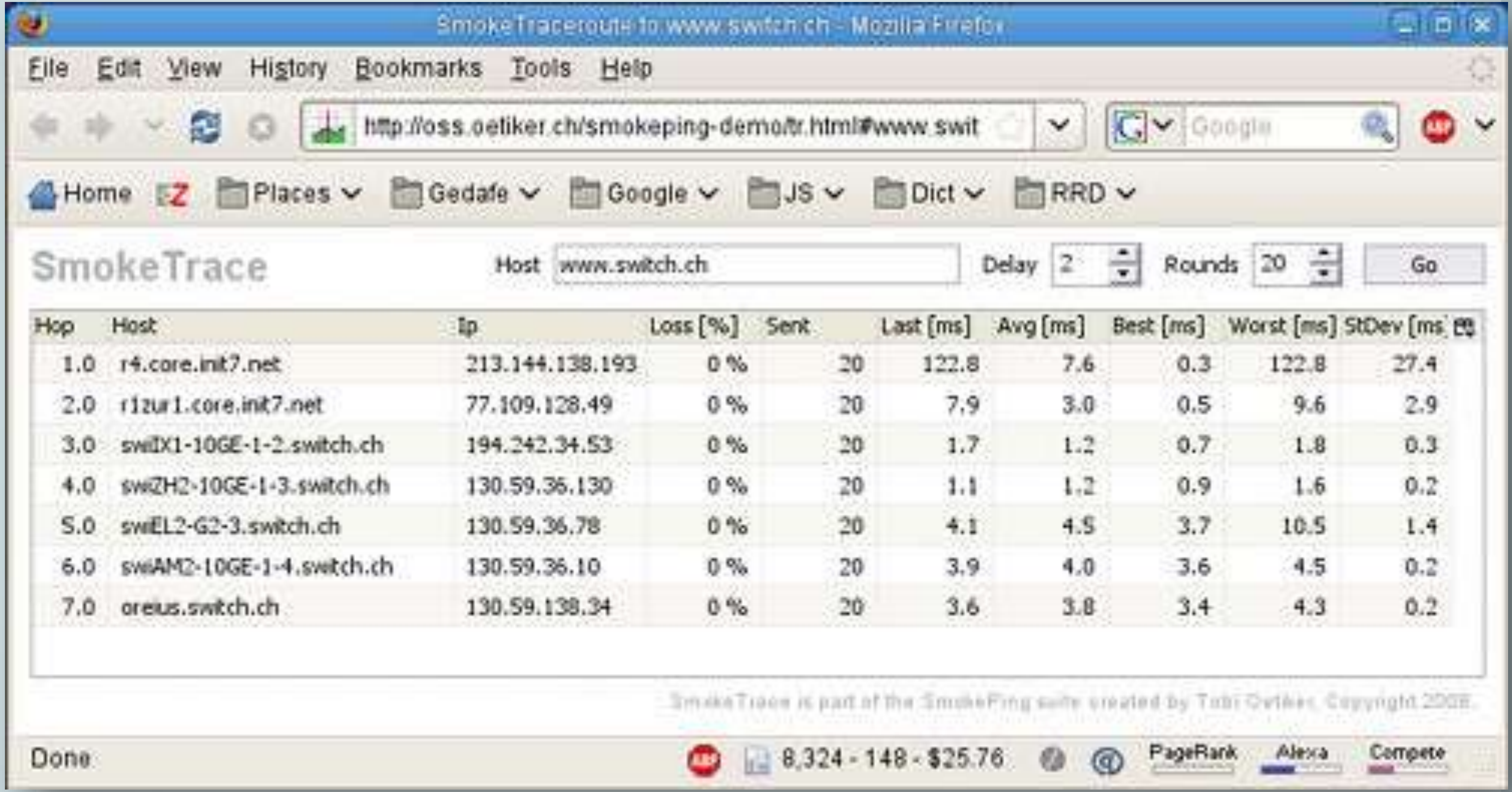
smokeping



```
median rtt:   34.6 ms avg   188.8 ms max   11.5 ms min   11.9 ms now   48.8 ms sd   708.1 m am/s
packet loss: 0.18 % avg   6.57 % 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: Thu Aug 30 18:01:22 2007 CEST
```

# Tools … SmokePing

smoke ping



SmokeTrace

Host www.switch.ch Delay 2 Rounds 20

| Hop | Host | Ip | Loss [%] | Sent | Last [ms] | Avg [ms] | Best [ms] | Worst [ms] | StDev [ms] |
|---|---|---|---|---|---|---|---|---|---|
| 1.0 | r4.core.init7.net | 213.144.138.193 | 0 % | 20 | 122.8 | 7.6 | 0.3 | 122.8 | 27.4 |
| 2.0 | r1zur1.core.init7.net | 77.109.128.49 | 0 % | 20 | 7.9 | 3.0 | 0.5 | 9.6 | 2.9 |
| 3.0 | swiIX1-10GE-1-2.switch.ch | 194.242.34.53 | 0 % | 20 | 1.7 | 1.2 | 0.7 | 1.8 | 0.3 |
| 4.0 | swiZH2-10GE-1-3.switch.ch | 130.59.36.130 | 0 % | 20 | 1.1 | 1.2 | 0.9 | 1.6 | 0.2 |
| 5.0 | swiEL2-G2-3.switch.ch | 130.59.36.78 | 0 % | 20 | 4.1 | 4.5 | 3.7 | 10.5 | 1.4 |
| 6.0 | swiAM2-10GE-1-4.switch.ch | 130.59.36.10 | 0 % | 20 | 3.9 | 4.0 | 3.6 | 4.5 | 0.2 |
| 7.0 | oreius.switch.ch | 130.59.138.34 | 0 % | 20 | 3.6 | 3.8 | 3.4 | 4.3 | 0.2 |

SmokeTrace is part of the SmokePing suite created by Tobi Oetiker, Copyright 2008.

# Components

□ Availability

□ Reliability

□ Performance

□ Configuration Mgmt & Monitoring

□ Network Forensic

□ Intrusion Detection …

□ ….

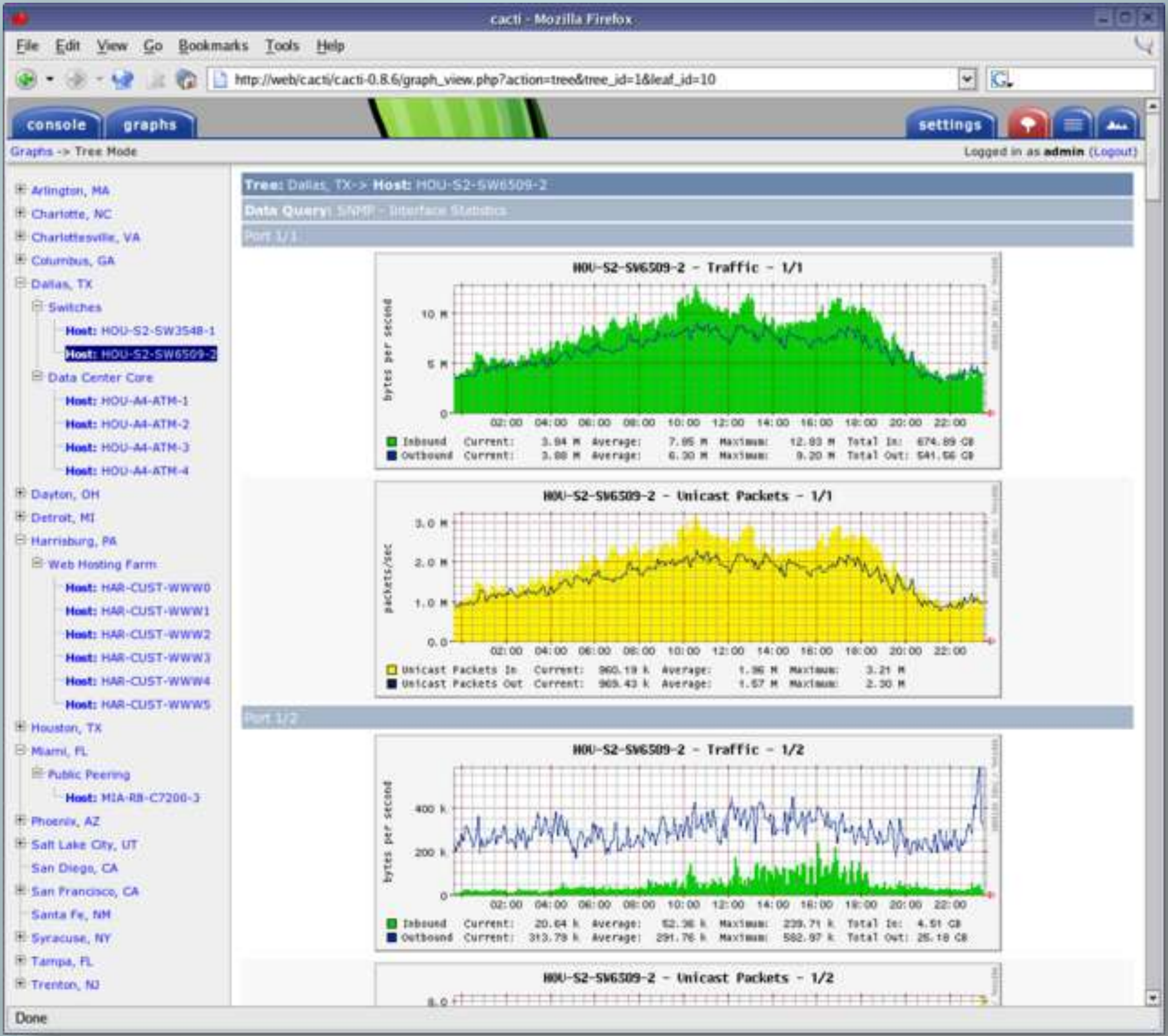
□ …..

□ Coordination

# Tools … Performance

- □ **Cacti/MRTG**
  - A tool to monitor, store and present network and system/server statistics
  - Designed around RRDTool with a special emphasis on the graphical interface
  - Almost all of Cacti's functionality can be configured via the Web.
  - Uses RRDtool, PHP and stores data in MySQL
  - Supports the use of SNMP and graphics with MRTG
  - Authentication Scheme
  - Large Network Deployment

# Tools … Cacti



http://web/cacti/cacti-0.8.6/graph_view.php?action=tree&tree_id=1&leaf_id=10

- Arlington, MA
- Charlotte, NC
- Charlottesville, VA
- Columbus, GA
- Dallas, TX
  - Switches
    - Host: HOU-S2-SW3548-1
    - Host: HOU-S2-SW6509-2
  - Data Center Core
    - Host: HOU-A4-ATM-1
    - Host: HOU-A4-ATM-2
    - Host: HOU-A4-ATM-3
    - Host: HOU-A4-ATM-4
- Dayton, OH
- Detroit, MI
- Harrisburg, PA
  - Web Hosting Farm
    - Host: HAR-CUST-WWW0
    - Host: HAR-CUST-WWW1
    - Host: HAR-CUST-WWW2
    - Host: HAR-CUST-WWW3
    - Host: HAR-CUST-WWW4
    - Host: HAR-CUST-WWW5
- Houston, TX
- Miami, FL
  - Public Peering
    - Host: MIA-RB-C7200-3
- Phoenix, AZ
- Salt Lake City, UT
- San Diego, CA
- San Francisco, CA
- Santa Fe, NM
- Syracuse, NY
- Tampa, FL
- Trenton, NJ

**Tree:** Dallas, TX-> **Host:** HOU-S2-SW6509-2

**Data Query:** SNMP - Interface Statistics

Port 1/1

HOU-S2-SW6509-2 - Traffic - 1/1

```
🟩 Inbound   Current:   3.94 M  Average:   7.05 M  Maximum:  12.83 M  Total In:  674.89 GB
■ Outbound  Current:   3.88 M  Average:   6.30 M  Maximum:   9.20 M  Total Out: 541.56 GB
```

HOU-S2-SW6509-2 - Unicast Packets - 1/1

```
□ Unicast Packets In   Current:  960.19 k  Average:   1.96 M  Maximum:   3.21 M
■ Unicast Packets Out  Current:  969.43 k  Average:   1.57 M  Maximum:   2.30 M
```

Port 1/2

HOU-S2-SW6509-2 - Traffic - 1/2

```
🟩 Inbound   Current:   20.64 k  Average:   52.36 k  Maximum:  239.71 k  Total In:   4.51 GB
■ Outbound  Current:  313.79 k  Average:  291.76 k  Maximum:  582.97 k  Total Out: 25.18 GB
```

HOU-S2-SW6509-2 - Unicast Packets - 1/2

Tools … Performance Visualization

# WeatherMap

Weathermap is a network visualization tool to take data you already have and show you an overview of your network in own customized map form/shape.

Tools ... Weathermap

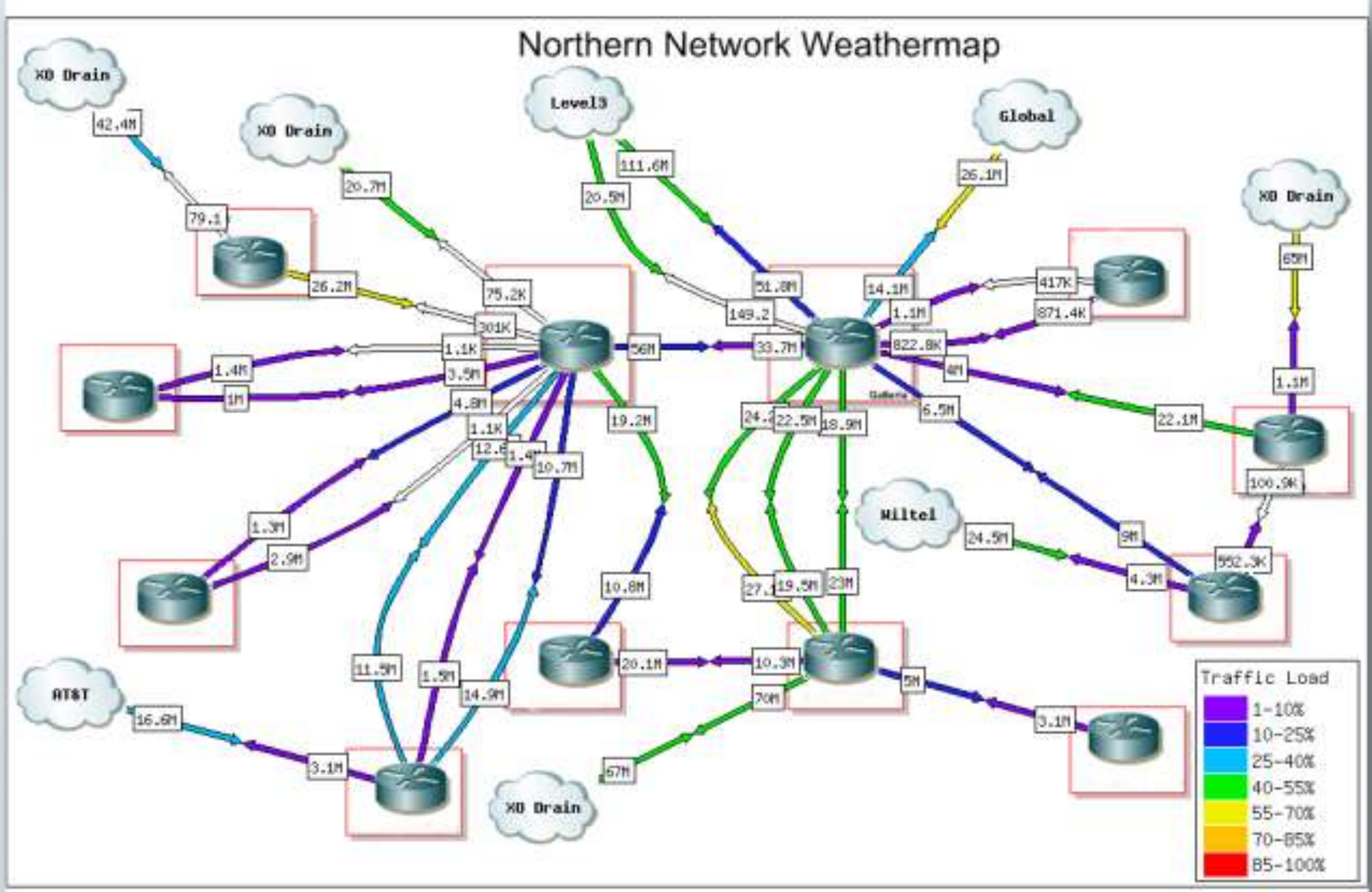
# KEY FEATURES:

**Cacti integration**: Weathermap comes with a Cactiplugin, allowing you to integrate network maps into the Cacti web UI, and provide a view of those maps to your users using Cacti's access control system. You don't *need* Cacti to use it though.

**Editor**: Weathermap includes a web-based editor to allow you to quickly 'sketch out' your map. It doesn't support all the feaures of Weathermap, but it doesn't get in their way either. You can use the web editor and a text editor together on the same map.

**Maintained and updated**: Weathermap is still being developed! I use this software myself, and as a result, find new ways *I'd* like to be able to do things. That means that bugs do get fixed, and features do get added.

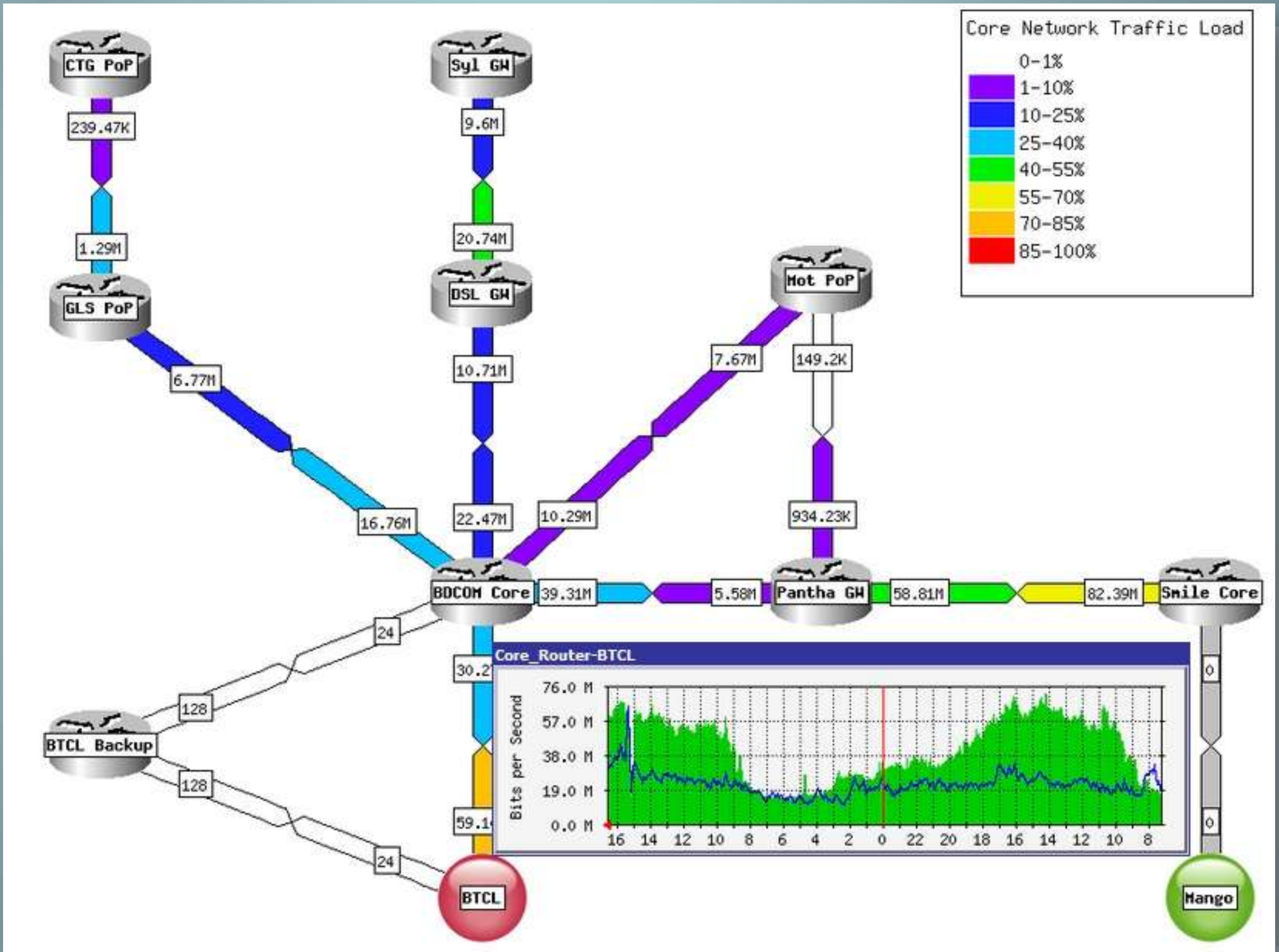
# Tools … Weathermap



Traffic Load

| | |
|---|---|
| 🟪 | 1-10% |
| 🟦 | 10-25% |
| 🟦 | 25-40% |
| 🟩 | 40-55% |
| 🟨 | 55-70% |
| 🟧 | 70-85% |
| 🟥 | 85-100% |

# Tools … Weathermap



# Components

□ Availability

□ Reliability

□ Performance

□ **Configuration Mgmt & Monitoring**

□ Network Forensic

□ Intrusion Detection …

□ ….

□ …..

□ Coordination

# Tools … Configuration Mgmt & Monitoring

**The ”Really Awesome New Cisco config Differ”**

- □ **Rancid**
  - Rancid is a configuration management tool that keeps track of changes in the configurations of any size network equipment (Cisco, HP, Juniper, Foundry, etc.). Works on routers and switches. Automates retrieval of the configurations and archives them as backup tool, audit tool, blame allocation.

# Tools … Rancid

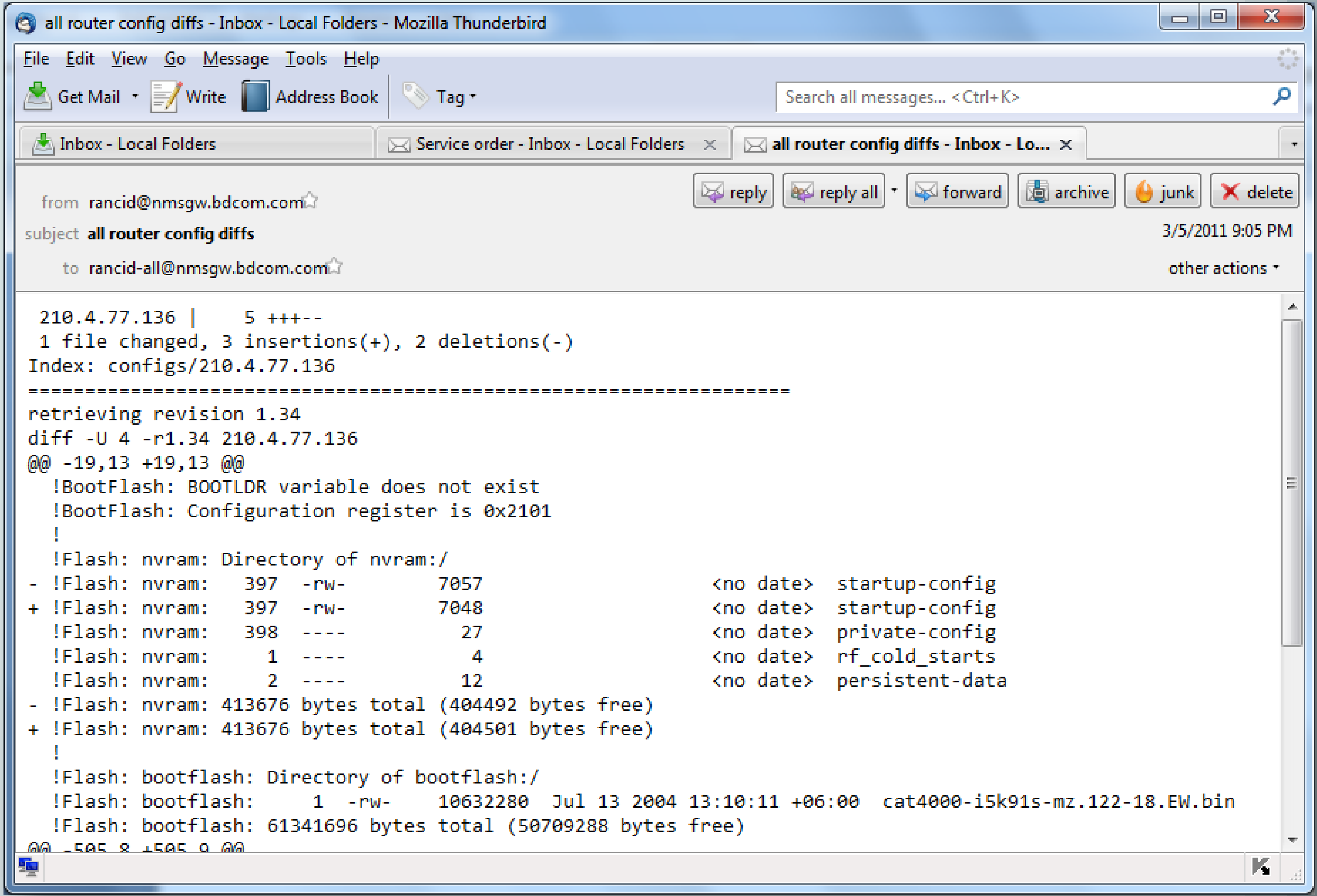
**The ”Really Awesome New Cisco config Differ”**

□ Rancid

The data is stored in a VCS (Version Control System) which keeps

- Track changes in the equipment configuration
- Track changes in the hardware (S/N, modules)
- Track version changes in the OS (IOS, CatOS versions)
- Find out what your colleagues have done without telling you!
- Recover from accidental configuration errors .

# Tools .. Rancid


all router config diffs - Inbox - Local Folders - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Tag
Search all messages... <Ctrl+K>
Inbox - Local Folders
Service order - Inbox - Local Folders
all router config diffs - Inbox - Lo...
reply
reply all
forward
archive
junk
delete
other actions

from rancid@nmsgw.bdcom.com

subject **all router config diffs**

to rancid-all@nmsgw.bdcom.com

3/5/2011 9:05 PM

```
 210.4.77.136 |     5 +++--
 1 file changed, 3 insertions(+), 2 deletions(-)
Index: configs/210.4.77.136
===================================================================
retrieving revision 1.34
diff -U 4 -r1.34 210.4.77.136
@@ -19,13 +19,13 @@
  !BootFlash: BOOTLDR variable does not exist
  !BootFlash: Configuration register is 0x2101
  !
  !Flash: nvram: Directory of nvram:/
- !Flash: nvram:   397  -rw-        7057                    <no date>  startup-config
+ !Flash: nvram:   397  -rw-        7048                    <no date>  startup-config
  !Flash: nvram:   398  ----          27                    <no date>  private-config
  !Flash: nvram:     1  ----           4                    <no date>  rf_cold_starts
  !Flash: nvram:     2  ----          12                    <no date>  persistent-data
- !Flash: nvram: 413676 bytes total (404492 bytes free)
+ !Flash: nvram: 413676 bytes total (404501 bytes free)
  !
  !Flash: bootflash: Directory of bootflash:/
  !Flash: bootflash:     1  -rw-    10632280  Jul 13 2004 13:10:11 +06:00  cat4000-i5k91s-mz.122-18.EW.bin
  !Flash: bootflash: 61341696 bytes total (50709288 bytes free)
@@ -505,8 +505,9 @@
```

# Components

- □ Availability
- □ Reliability
- □ Performance
- □ Configuration Mgmt & Monitoring
- □ Network Forensic
- □ Intrusion Detection …
- □ ….
- □ …..
- □ Coordination

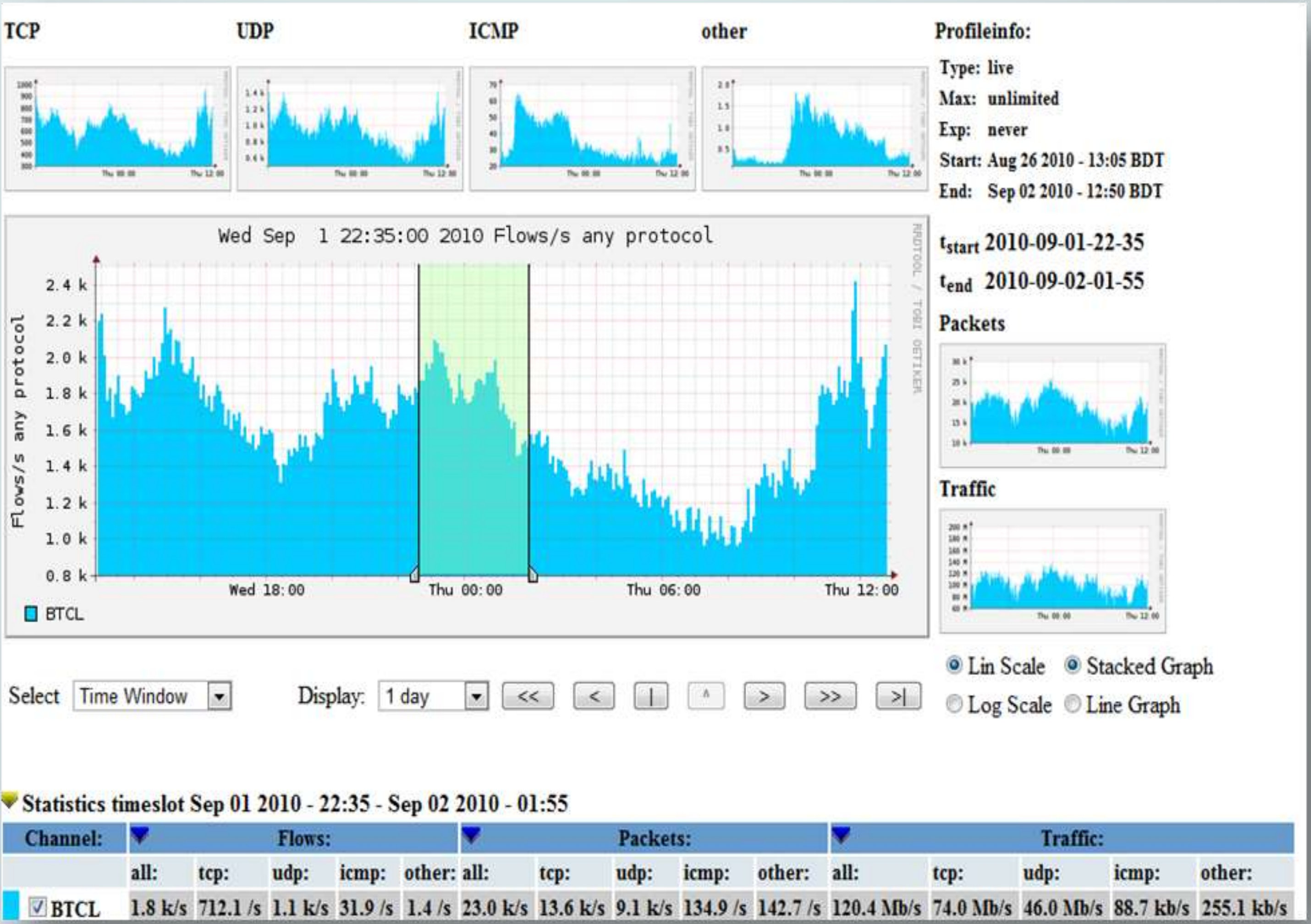
# Tools … Net Forensic

- **Network Flow Analysis Tool**
  - NetFlow (C),
  - cflowd (F),
  - FlowScan (F),
  - Sniffer Pro (C),
  - argus (F),
  - i-Flow (C)
  - NFSen (F)

# Tools … NFSen

- **Network Flow Analysis Tool**
  - **NFSen**
    - Display netflow data: Flows, Packets and Bytes using RRD (Round Robin Database).
    - Easily navigate through the netflow data.
    - Process the netflow data within the specified time span.
    - Create history as well as continuous profiles.
    - Set alerts, based on various conditions.

# Tools … NFSen



**Profileinfo:**

Type: live

Max: unlimited

Exp: never

Start: Aug 26 2010 - 13:05 BDT

End: Sep 02 2010 - 12:50 BDT

$t_{start}$ 2010-09-01-22-35

$t_{end}$ 2010-09-02-01-55

● Lin Scale ● Stacked Graph

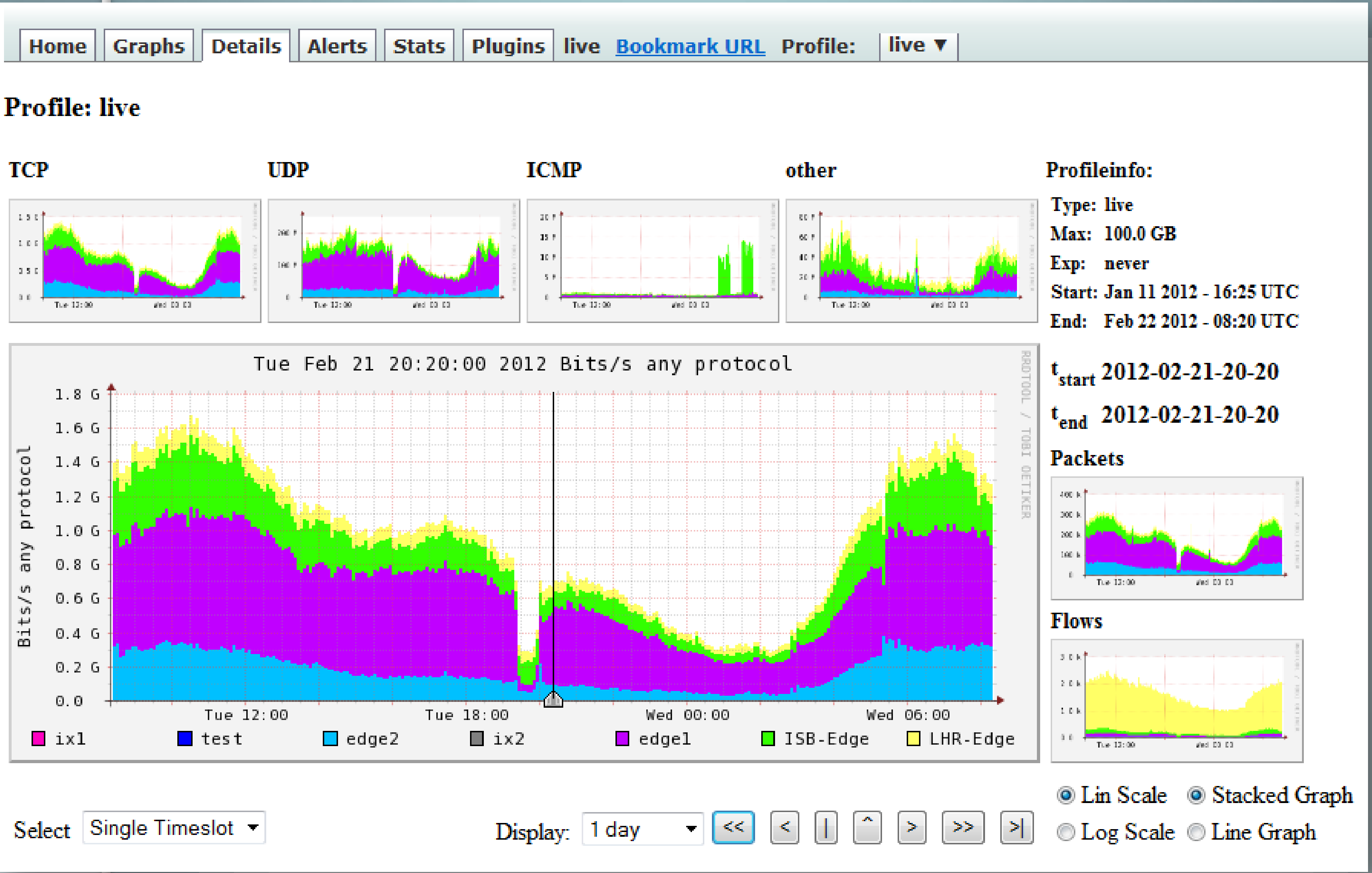
○ Log Scale ○ Line Graph

Select: Time Window

Display: 1 day

Statistics timeslot Sep 01 2010 - 22:35 - Sep 02 2010 - 01:55

| Channel: | Flows: | | | | | Packets: | | | | | Traffic: | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: | all: | tcp: | udp: | icmp: | other: |
| ☑ BTCL | 1.8 k/s | 712.1 /s | 1.1 k/s | 31.9 /s | 1.4 /s | 23.0 k/s | 13.6 k/s | 9.1 k/s | 134.9 /s | 142.7 /s | 120.4 Mb/s | 74.0 Mb/s | 46.0 Mb/s | 88.7 kb/s | 255.1 kb/s |



## Profile: live

**Profileinfo:**

Type: live

Max: 100.0 GB

Exp: never

Start: Jan 11 2012 - 16:25 UTC

End: Feb 22 2012 - 08:20 UTC

$t_{start}$ 2012-02-21-20-20

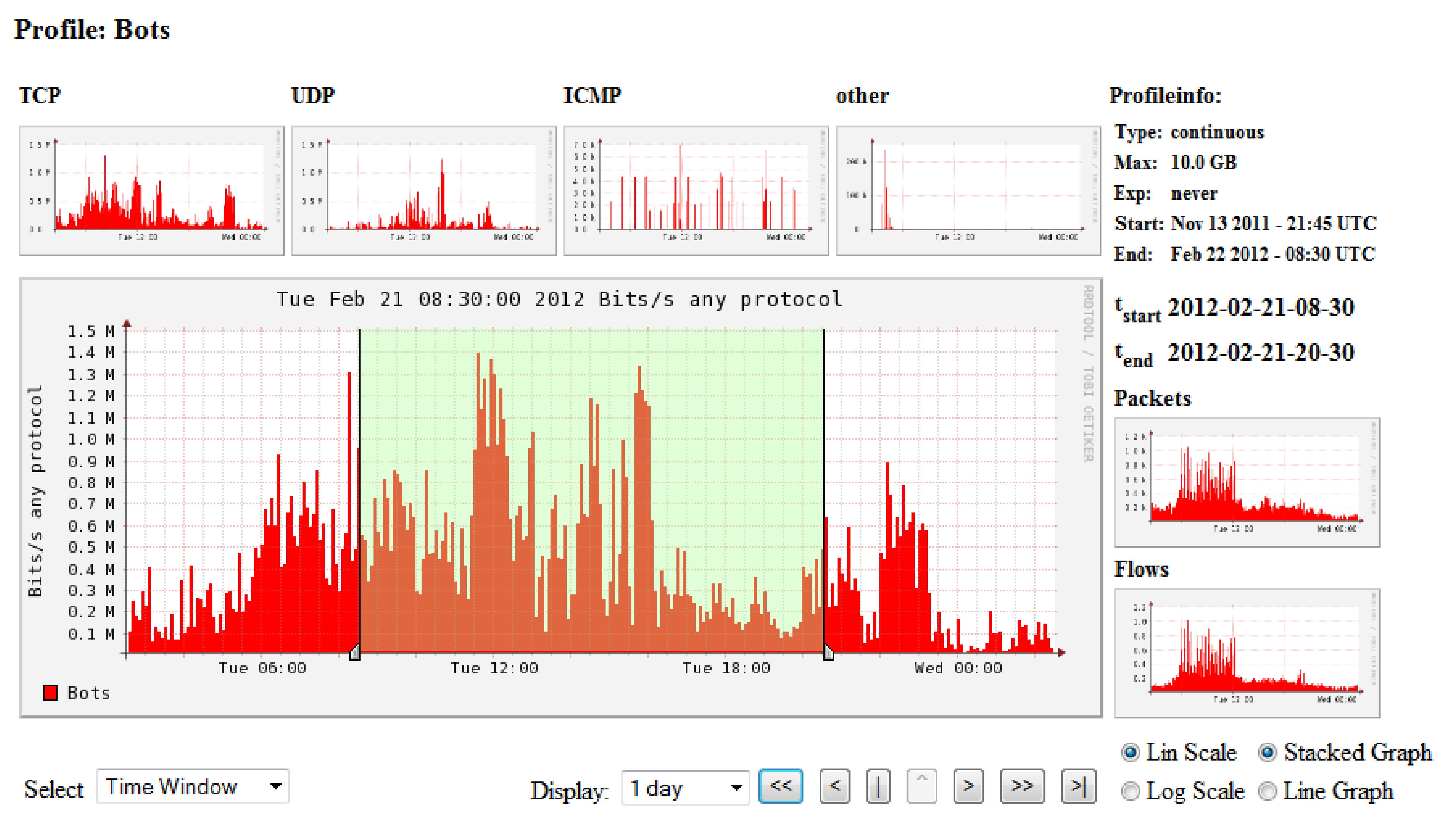
$t_{end}$ 2012-02-21-20-20

● Lin Scale ● Stacked Graph

○ Log Scale ○ Line Graph

Select: Single Timeslot

Display: 1 day



Profile: Bots

TCP UDP ICMP other

Profileinfo:

Type: continuous
Max: 10.0 GB
Exp: never
Start: Nov 13 2011 - 21:45 UTC
End: Feb 22 2012 - 08:30 UTC

$t_{start}$ 2012-02-21-08-30
$t_{end}$ 2012-02-21-20-30

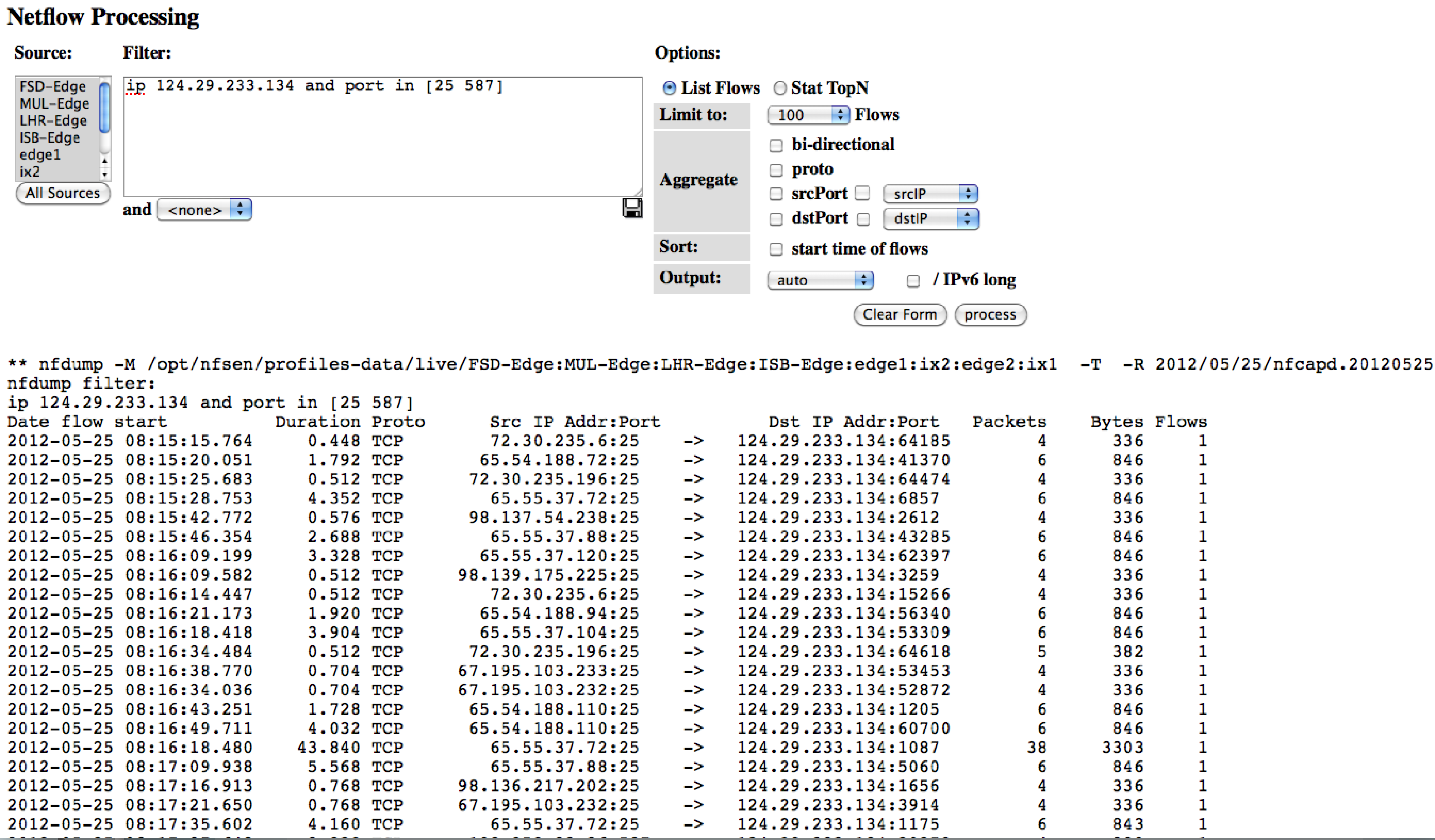
Packets

Flows

Tue Feb 21 08:30:00 2012 Bits/s any protocol

Select: Time Window
Display: 1 day

● Lin Scale ● Stacked Graph
○ Log Scale ○ Line Graph



## Netflow Processing

**Source:** FSD-Edge, MUL-Edge, LHR-Edge, ISB-Edge, edge1, ix2

**Filter:**

```
ip 124.29.233.134 and port in [25 587]
```

and <none>

**Options:**

● List Flows ○ Stat TopN

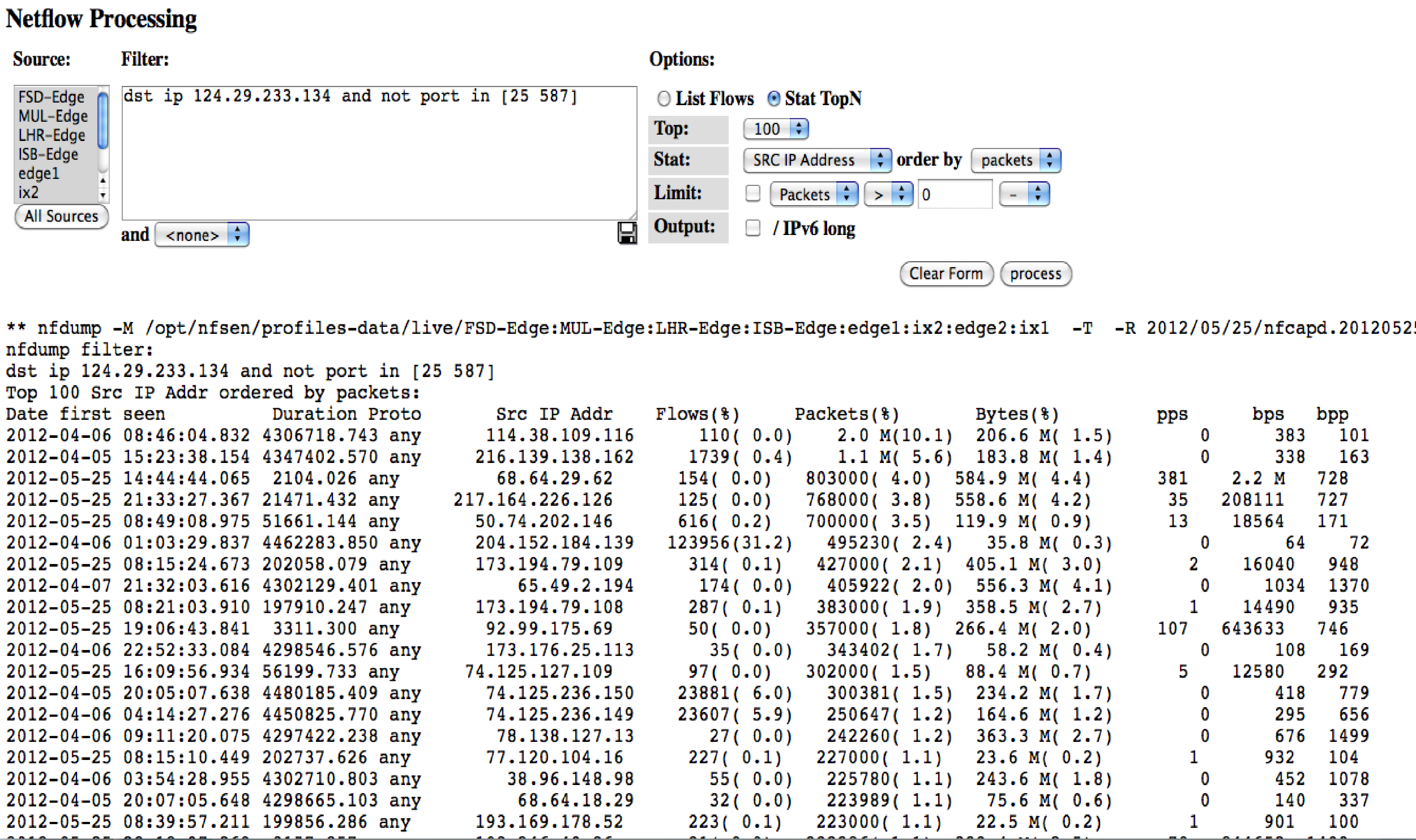
**Limit to:** 100 Flows

**Aggregate** □ bi-directional □ proto □ srcPort □ srcIP □ dstPort □ dstIP

**Sort:** □ start time of flows

**Output:** auto □ / IPv6 long

```
** nfdump -M /opt/nfsen/profiles-data/live/FSD-Edge:MUL-Edge:LHR-Edge:ISB-Edge:edge1:ix2:edge2:ix1  -T  -R 2012/05/25/nfcapd.20120525
nfdump filter:
ip 124.29.233.134 and port in [25 587]
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2012-05-25 08:15:15.764     0.448 TCP       72.30.235.6:25    ->   124.29.233.134:64185         4      336     1
2012-05-25 08:15:20.051     1.792 TCP      65.54.188.72:25    ->   124.29.233.134:41370         6      846     1
2012-05-25 08:15:25.683     0.512 TCP     72.30.235.196:25    ->   124.29.233.134:64474         4      336     1
2012-05-25 08:15:28.753     4.352 TCP      65.55.37.72:25     ->   124.29.233.134:6857          6      846     1
2012-05-25 08:15:42.772     0.576 TCP     98.137.54.238:25    ->   124.29.233.134:2612          4      336     1
2012-05-25 08:15:46.354     2.688 TCP      65.55.37.88:25     ->   124.29.233.134:43285         6      846     1
2012-05-25 08:16:09.199     3.328 TCP      65.55.37.120:25    ->   124.29.233.134:62397         6      846     1
2012-05-25 08:16:09.582     0.512 TCP    98.139.175.225:25    ->   124.29.233.134:3259          4      336     1
2012-05-25 08:16:14.447     0.512 TCP       72.30.235.6:25    ->   124.29.233.134:15266         4      336     1
2012-05-25 08:16:21.173     1.920 TCP      65.54.188.94:25    ->   124.29.233.134:56340         6      846     1
2012-05-25 08:16:18.418     3.904 TCP      65.55.37.104:25    ->   124.29.233.134:53309         6      846     1
2012-05-25 08:16:34.484     0.512 TCP     72.30.235.196:25    ->   124.29.233.134:64618         5      382     1
2012-05-25 08:16:38.770     0.704 TCP    67.195.103.233:25    ->   124.29.233.134:53453         4      336     1
2012-05-25 08:16:34.036     0.704 TCP    67.195.103.232:25    ->   124.29.233.134:52872         4      336     1
2012-05-25 08:16:43.251     1.728 TCP     65.54.188.110:25    ->   124.29.233.134:1205          6      846     1
2012-05-25 08:16:49.711     4.032 TCP     65.54.188.110:25    ->   124.29.233.134:60700         6      846     1
2012-05-25 08:16:18.480    43.840 TCP      65.55.37.72:25     ->   124.29.233.134:1087         38     3303     1
2012-05-25 08:17:09.938     5.568 TCP      65.55.37.88:25     ->   124.29.233.134:5060          6      846     1
2012-05-25 08:17:16.913     0.768 TCP    98.136.217.202:25    ->   124.29.233.134:1656          4      336     1
2012-05-25 08:17:21.650     0.768 TCP    67.195.103.232:25    ->   124.29.233.134:3914          4      336     1
2012-05-25 08:17:35.602     4.160 TCP      65.55.37.72:25     ->   124.29.233.134:1175          6      843     1
```



## Netflow Processing

**Source:** FSD-Edge, MUL-Edge, LHR-Edge, ISB-Edge, edge1, ix2 — All Sources

**Filter:**

```
dst ip 124.29.233.134 and not port in [25 587]
```

and <none>

**Options:**

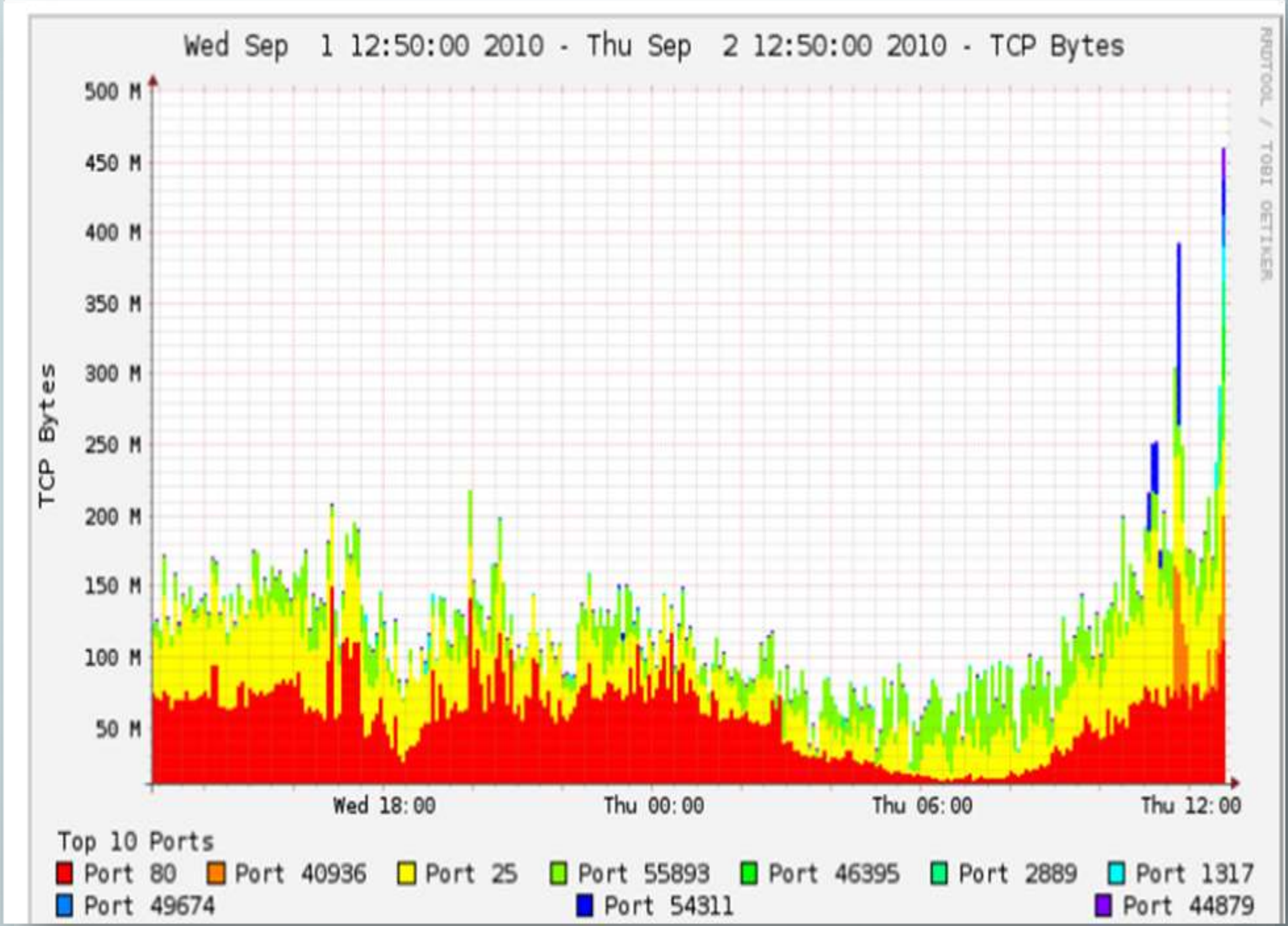
○ List Flows ● Stat TopN

| | |
|---|---|
| **Top:** | 100 |
| **Stat:** | SRC IP Address **order by** packets |
| **Limit:** | □ Packets > 0 - |
| **Output:** | □ / IPv6 long |

Clear Form   process

```
** nfdump -M /opt/nfsen/profiles-data/live/FSD-Edge:MUL-Edge:LHR-Edge:ISB-Edge:edge1:ix2:edge2:ix1  -T  -R 2012/05/25/nfcapd.201205
nfdump filter:
dst ip 124.29.233.134 and not port in [25 587]
Top 100 Src IP Addr ordered by packets:
Date first seen          Duration Proto       Src IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2012-04-06 08:46:04.832 4306718.743 any     114.38.109.116      110( 0.0)    2.0 M(10.1)  206.6 M( 1.5)        0      383   101
2012-04-05 15:23:38.154 4347402.570 any    216.139.138.162     1739( 0.4)    1.1 M( 5.6)  183.8 M( 1.4)        0      338   163
2012-05-25 14:44:44.065  2104.026 any        68.64.29.62      154( 0.0)   803000( 4.0)  584.9 M( 4.4)      381    2.2 M   728
2012-05-25 21:33:27.367 21471.432 any    217.164.226.126      125( 0.0)   768000( 3.8)  558.6 M( 4.2)       35   208111   727
2012-05-25 08:49:08.975 51661.144 any      50.74.202.146      616( 0.2)   700000( 3.5)  119.9 M( 0.9)       13    18564   171
2012-04-06 01:03:29.837 4462283.850 any    204.152.184.139   123956(31.2)   495230( 2.4)   35.8 M( 0.3)        0       64    72
2012-05-25 08:15:24.673 202058.079 any     173.194.79.109      314( 0.1)   427000( 2.1)  405.1 M( 3.0)       2    16040   948
2012-04-07 21:32:03.616 4302129.401 any        65.49.2.194      174( 0.0)   405922( 2.0)  556.3 M( 4.1)        0     1034  1370
2012-05-25 08:21:03.910 197910.247 any     173.194.79.108      287( 0.1)   383000( 1.9)  358.5 M( 2.7)       1    14490   935
2012-05-25 19:06:43.841  3311.300 any       92.99.175.69       50( 0.0)   357000( 1.8)  266.4 M( 2.0)      107   643633   746
2012-04-06 22:52:33.084 4298546.576 any     173.176.25.113       35( 0.0)   343402( 1.7)   58.2 M( 0.4)        0      108   169
2012-05-25 16:09:56.934 56199.733 any     74.125.127.109       97( 0.0)   302000( 1.5)   88.4 M( 0.7)        5    12580   292
2012-04-05 20:05:07.638 4480185.409 any     74.125.236.150    23881( 6.0)   300381( 1.5)  234.2 M( 1.7)        0      418   779
2012-04-06 04:14:27.276 4450825.770 any     74.125.236.149    23607( 5.9)   250647( 1.2)  164.6 M( 1.2)        0      295   656
2012-04-06 09:11:20.075 4297422.238 any      78.138.127.13       27( 0.0)   242260( 1.2)  363.3 M( 2.7)        0      676  1499
2012-05-25 08:15:10.449 202737.626 any      77.120.104.16      227( 0.1)   227000( 1.1)   23.6 M( 0.2)       1      932   104
2012-04-06 03:54:28.955 4302710.803 any       38.96.148.98       55( 0.0)   225780( 1.1)  243.6 M( 1.8)        0      452  1078
2012-04-05 20:07:05.648 4298665.103 any        68.64.18.29       32( 0.0)   223989( 1.1)   75.6 M( 0.6)        0      140   337
2012-05-25 08:39:57.211 199856.286 any     193.169.178.52      223( 0.1)   223000( 1.1)   22.5 M( 0.2)       1      901   100
```

# Tools … NFSen (Port Tracker)



# Tools .. NFSen (Port Tracker)

| | TCP | | | | | | UDP | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Flows | | Packets | | Bytes | | Flows | | Packets | | Bytes | |
| Rank | Port | Count | Port | Count | Port | Count | Port | Count | Port | Count | Port | Count |
| 1 | 80 | 39029 | 80 | 570630 | 80 | 111021671 | 53 | 116671 | 53 | 150335 | 12610 | 142186426 |
| 2 | 445 | 27833 | 25 | 83140 | 40936 | 88004359 | 6881 | 2388 | 12610 | 99433 | 28712 | 101344390 |
| 3 | 135 | 24572 | 40936 | 66203 | 25 | 52612168 | 39792 | 2276 | 28712 | 70901 | 40493 | 93146942 |
| 4 | 25 | 7881 | 445 | 53175 | 55893 | 43525223 | 15507 | 1904 | 40493 | 65155 | 46886 | 27824516 |
| 5 | 23 | 6761 | 135 | 49066 | 46395 | 39079355 | 43040 | 1611 | 15699 | 46682 | 57563 | 26436088 |
| 6 | 3128 | 4786 | 55893 | 37615 | 2889 | 30261886 | 60928 | 1588 | 1416 | 40540 | 62390 | 25767022 |
| 7 | 443 | 2999 | 46395 | 35068 | 1317 | 24692504 | 51012 | 1573 | 57563 | 37794 | 54505 | 25550351 |
| 8 | 22 | 2517 | 22 | 27489 | 49674 | 23472247 | 61295 | 1447 | 34018 | 37747 | 55893 | 23548341 |
| 9 | 9415 | 1275 | 443 | 26468 | 54311 | 23342821 | 5060 | 1309 | 21694 | 24942 | 40633 | 22940400 |
| **10** | **8080** | **1081** | **21651** | **25614** | **44879** | **23306526** | **49665** | **1225** | **46886** | **19468** | **40403** | **19544859** |

# Components

- □ Availability
- □ Reliability
- □ Performance
- □ Configuration Mgmt & Monitoring
- □ Network Forensic
- □ Intrusion Detection …
- □ ….
- □ …..
- □ Coordination

# Tools … IDS & IPS

**Computer Security is not something that you can just add on when you need it.**

Proper planning, installation, monitoring and maintenance all become part of a successful IDS/IPS implementation.

□ Tri-Sentry (Host Sentry, NetSentry, Service Sentry)

□ Nessus, Snort, nmap, Nikto, Tripwire,Samhain, Fcheck

□ Checkpoint, Cisco IPS, VCC/Tripwire, F5, Big Iron, Juniper

□ UTM (Cyberoam, Barracuda)

BIG BOYS WILL DISCUSS ….

# Components

- □ Availability
- □ Reliability
- □ Performance
- □ Configuration Mgmt & Monitoring
- □ Network Forensic
- □ Intrusion Detection …
- □ ….
- □ …..
- □ Coordination

# Tools … Collaboration

So, we have many Open Source/Commercial deployments already to monitor our network.

All the programs can generate alert/alarm on fault detection.

Need to centralize all the information.

We need to collaborate these programs

Need NOC

Its not a big Room/House – it's a software

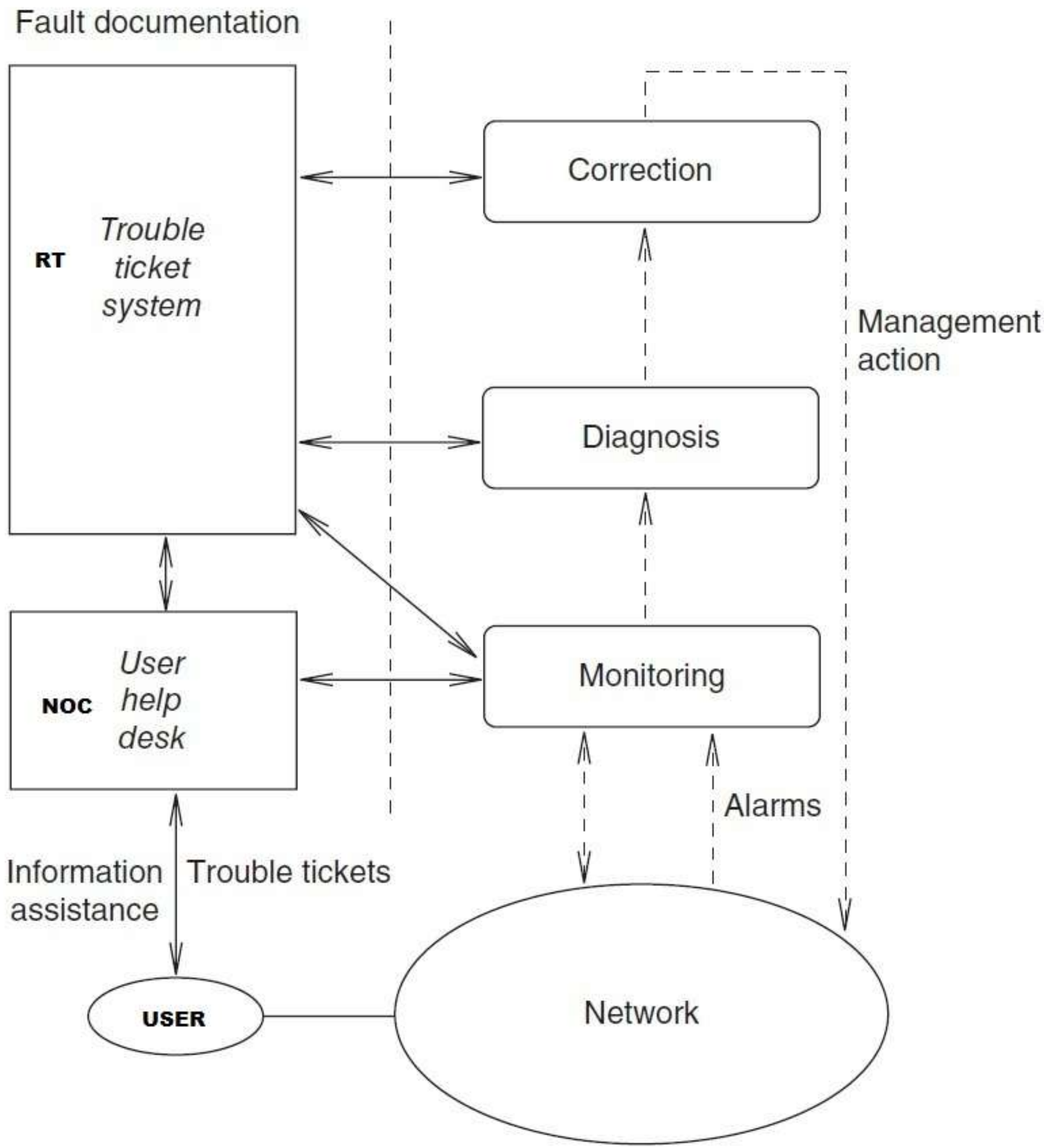
Its –RT (the ticketing system)

Tools … RT

## Request Tracker

- **RT** is a battle-tested issue tracking system which thousands of organizations use for
  - bug tracking,
  - help desk ticketing,
  - customer service,
  - workflow processes,
  - change management,
  - network operations,
  - And so on ..

# Tools … RT


Fault documentation
RT
Trouble ticket system
Correction
Management action
Diagnosis
Monitoring
NOC
User help desk
Alarms
Information assistance
Trouble tickets
USER
Network

# Tools … RT

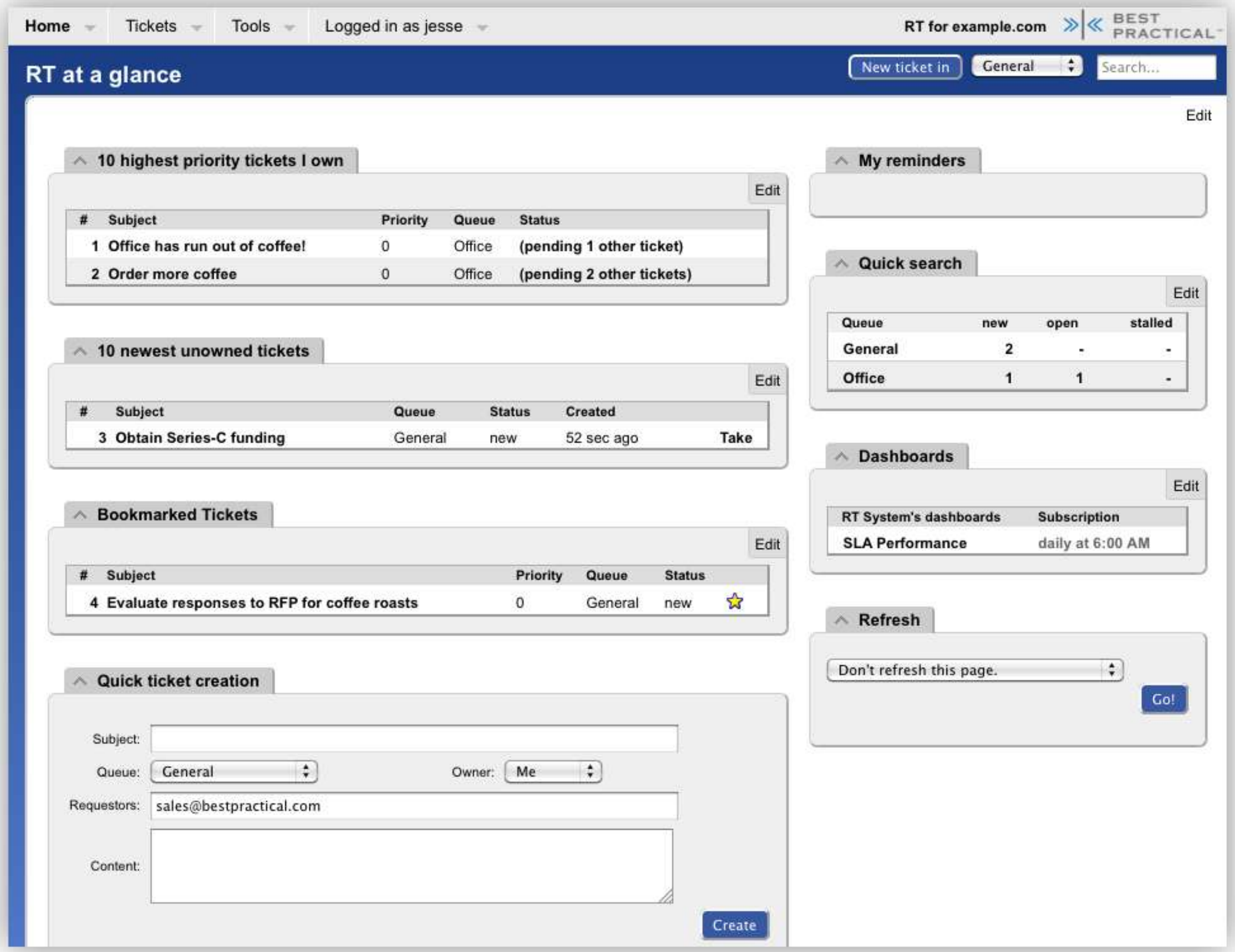
## Request Tracker

Whenever, wherever and however there is a problem in the network the relevant monitoring software will send a ticket directly to RT system and system admins will know immediately via email or SMS. This automation will keep track of the SLA. RT has its own Help Desk system and escalation procedure.

# Tools .. RT

- Why are they important?
  - Track all events, failures and issues
- Focal point for help desk communication
- Use it to track all communications
  - Both internal and external
- Events originating from the outside:
  - customer complaints
- Events originating from the inside:
  - System outages (direct or indirect)
  - Planned maintenance, upgrades, etc.

# Tools … RT



## RT at a glance

### 10 highest priority tickets I own

| # | Subject | Priority | Queue | Status |
|---|---|---|---|---|
| 1 | Office has run out of coffee! | 0 | Office | (pending 1 other ticket) |
| 2 | Order more coffee | 0 | Office | (pending 2 other tickets) |

### 10 newest unowned tickets

| # | Subject | Queue | Status | Created | |
|---|---|---|---|---|---|
| 3 | Obtain Series-C funding | General | new | 52 sec ago | Take |

### Bookmarked Tickets

| # | Subject | Priority | Queue | Status | |
|---|---|---|---|---|---|
| 4 | Evaluate responses to RFP for coffee roasts | 0 | General | new | ☆ |

### Quick ticket creation

Subject:

Queue: General

Owner: Me

Requestors: sales@bestpractical.com

Content:

### My reminders

### Quick search

| Queue | new | open | stalled |
|---|---|---|---|
| General | 2 | - | - |
| Office | 1 | 1 | - |

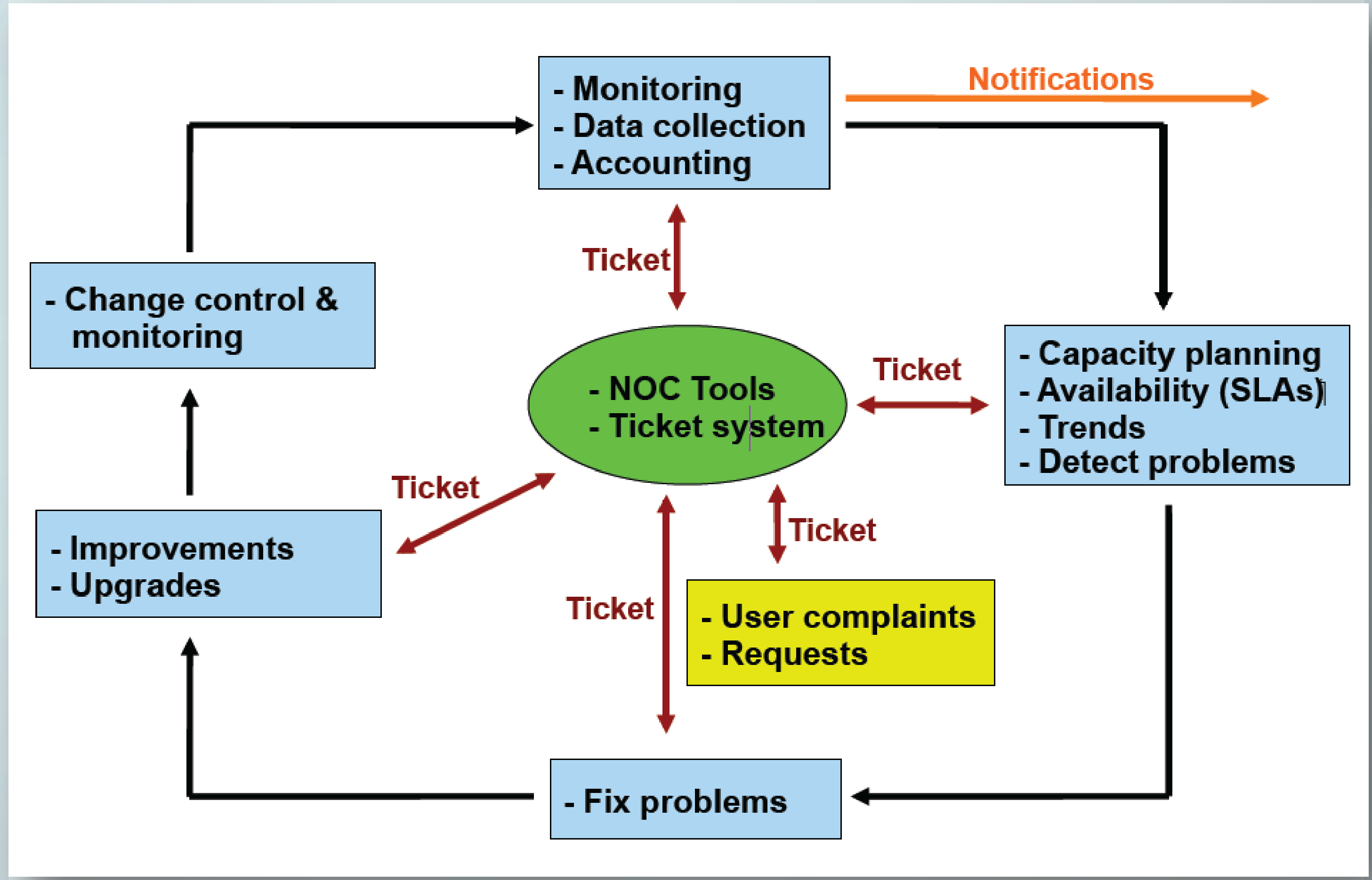
### Dashboards

| RT System's dashboards | Subscription |
|---|---|
| SLA Performance | daily at 6:00 AM |

### Refresh

Don't refresh this page.

# Tools ... RT



- Monitoring
- Data collection
- Accounting

Notifications

- Change control & monitoring

- NOC Tools
- Ticket system

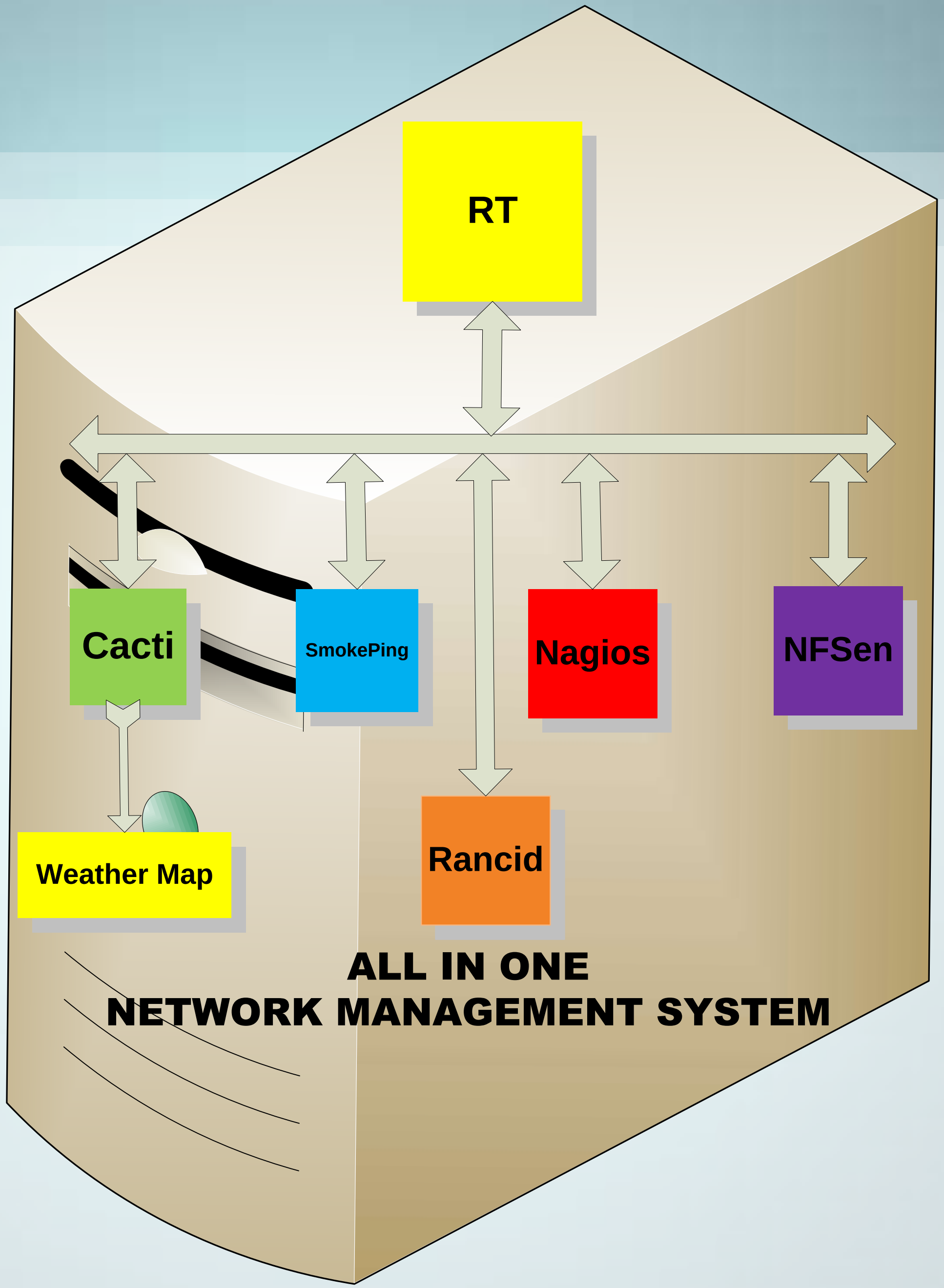
- Capacity planning
- Availability (SLAs)
- Trends
- Detect problems

- Improvements
- Upgrades

- User complaints
- Requests

- Fix problems

# Conclusion



RT

Cacti

SmokePing

Nagios

NFSen

Weather Map

Rancid

ALL IN ONE
NETWORK MANAGEMENT SYSTEM

# What did we learn?

- We learned some of the advantages of having a well-managed network
- We learned the features of some Open Source Network Monitoring tools
  - Nagios for monitoring network elements and servers
  - Smokeping for measuring latency in your network reliability measurement
  - Cacti/MRTG & Weathermap for graphing traffic and other statistics
  - RANCID for the backup of configs with version control
  - NFSen for network forensic
  -
- We tied them all in a simple working Environment - RT

# What we did not cover

- So much more...

- All this software has many more features and is extensible
  - Read docs, forums, examples
  - Read the source code if you can
  - Ask questions, try it out

- There's commercial alternatives, and alternatives by hardware vendors
  - Compare the features, ask for a test version
  - Only because it costs money, it's not necessarily better/easier to manage (but maybe it is)
  - It all depends on YOUR needs
  - Support is also available for open-source tools

# What we did not cover

There's more network management/monitoring than the tools we covered, you can try the following tools (in no particular order

- Visualize network designs with tools like **Dia** or **Microsoft Visio** or discover it automatically with **Network Weathermap via Cacti**
- Manage/secure who has router access with RADIUS or TACACS servers like Shrubbery's **TACACS+** daemon or **Freeradius**
- Sniff and analyze Network traffic using **Wireshark**
- Install intrusion detection systems like **SNORT**
- Use a portscanner like **nmap** to find open ports or a scanner like **Nessus** to find potential vulnerabilities in your network

# We're still not done

- Use a Wiki or Content Management system for your documentation like **trac** or **TWiki**
- Use **Netdot** and **Netdisco** to manage your addressing equipment
- Manage code for your tools or other data which changes using a versioning system like **CVS** or **Subversion** (we mentioned it in RANCID)

# Some more.......

## Performance

- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

## Ticketing

- RT, Trac, Redmine

## Change Mgmt

- Mercurial
- Rancid (routers)
- RCS
- Subversion

## Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

And that's not all!!!

## Net Management

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

???