AfNOG-2013

Monitoring of IP Services

Ayitey Bulley

Material generously borrowed from the NSRC NME course

Introduction

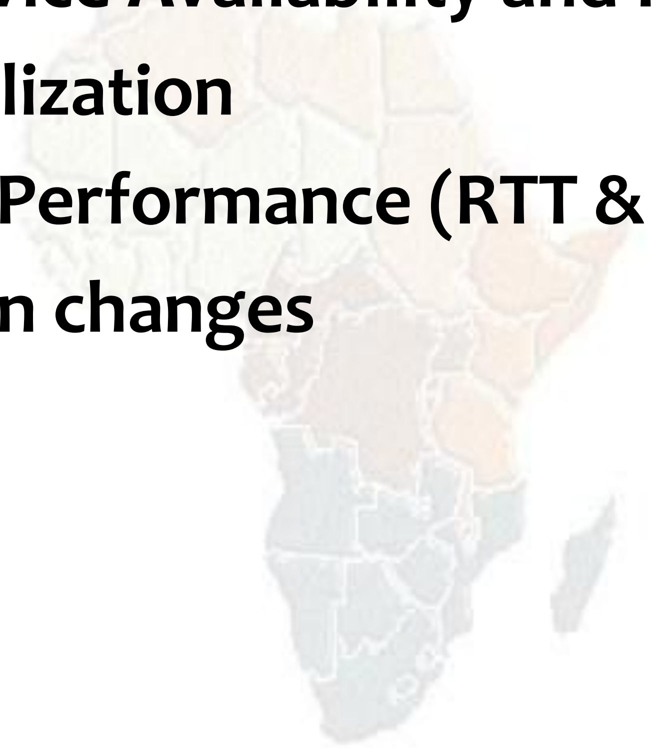
- To monitor or monitoring generally means to be aware of the state of a system.
- To observe a situation for any changes which may occur over time, using a monitor or measuring device of some sort.
- The term network monitoring describes the use of a system that constantly monitors a computer network for faults and notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

Monitoring Types

- Application Performance Monitoring
- Environmental Monitoring
- Network Monitoring
- System Monitoring
- Website Monitoring

What do we Monitor?

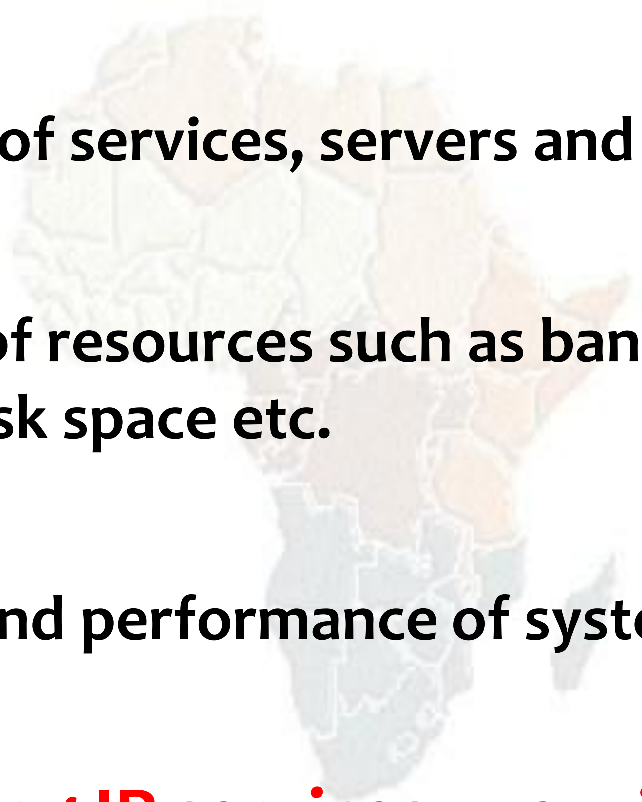
- Systems/Service Availability and Reliability
- Resource Utilization
- Reliability & Performance (RTT & Throughput)
- Configuration changes



Why Monitor?

- Deliver on targets (KPIs/SLAs)
- Early detection and fault resolution (MTTR)
- Accurately report on the state of the systems being managed

Monitoring Tools



- Nagios
  - Availability of services, servers and network devices.
- Cacti
  - Utilization of resources such as bandwidth, cpu, memory, disk space etc.
- Smokeping
  - Reliability and performance of systems and services.

- For monitoring IP services, we will focus on monitoring availability (Nagios) and reliability (Smokeping)

Nagios

- Nagios actively monitors the availability of devices and services
  - Availability of services, servers and network devices.
- Possibly the most used open source network monitoring software.
- Sends alerts and/or triggers alerts
- Logs history and generates SLA reports
- Can support up to thousands of devices and services.

Perspective on Availability?

Availability %	Downtime per Year	Downtime per Month	Downtime per Week
90% ("one nine")	36.5 days	72 hours	16.8 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds

Nagios – FreeBSD Installation

- Dependencies:
  - MySQL , Apache & PHP
- Install nagios from ports:

```
# cd /usr/ports/net-mgmt/nagios
# make all install clean
```

- Key directories:

```
/usr/local/etc/nagios
/usr/local/etc/nagios/objects
/usr/local/libexec/nagios
/usr/local/www/nagios
```

- Nagios web interface sample is here:
  - http://noc.sse.ws.afnog.org/nagios

Nagios – Architecture

- Plugins are used to verify the state of devices & services.
  - Small, self-contained applications which make a single connection to test a service then quit
  - Return OK, Warning, Critical or Unknown
  - Many plugins supplied, even more available
    - http://exchange.nagios.org
    - http://nagiosplugins.org
- Data storage: plain text files
- Data visualisation: CGI web interface
- Configuration: plain text files

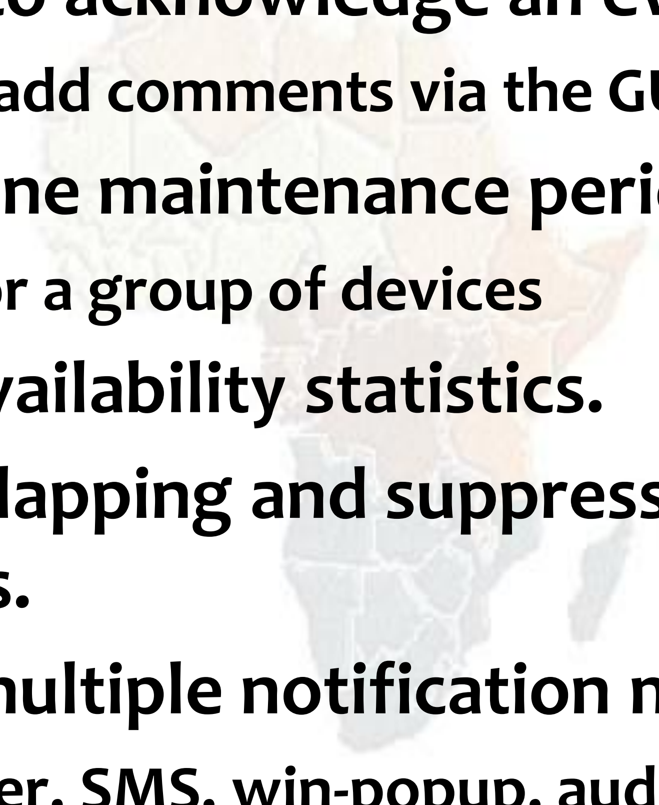
Nagios – Configuration Files

- **Located in /usr/local/etc/nagios:**
  - **cgi.cfg**
    - **Controls the web interface and security options**
  - **nagios.cfg**
    - **Main configuration file**
  - **resource.cfg**
    - **Used to specify an optional resource file that can contain $USERn$ macro definitions.**
  - **objects/**
    - **All other configuration files go here.**

Nagios – Configuration Files

- The /usr/local/etc/nagios/objects directory:
  - commands.cfg
    - The commands that nagios uses for notifications
  - contacts.cfg
    - Users and groups
  - localhost.cfg
    - Definition of the nagios host
  - printer.cfg, switch.cfg
    - Definition of printers and switches
  - templates.cfg
    - Sample object templates
  - timeperiods.cfg
    - Defines when to check the state of objects

Nagios – Features



- Allows you to acknowledge an event.
  - A user can add comments via the GUI
- You can define maintenance periods
  - By device or a group of devices
- Maintains availability statistics.
- Can detect flapping and suppress additional notifications.
- Allows for multiple notification methods:
  - e-mail, pager, SMS, win-popup, audio, etc...
- Allows you to define notification levels for escalation

Nagios – Exercise

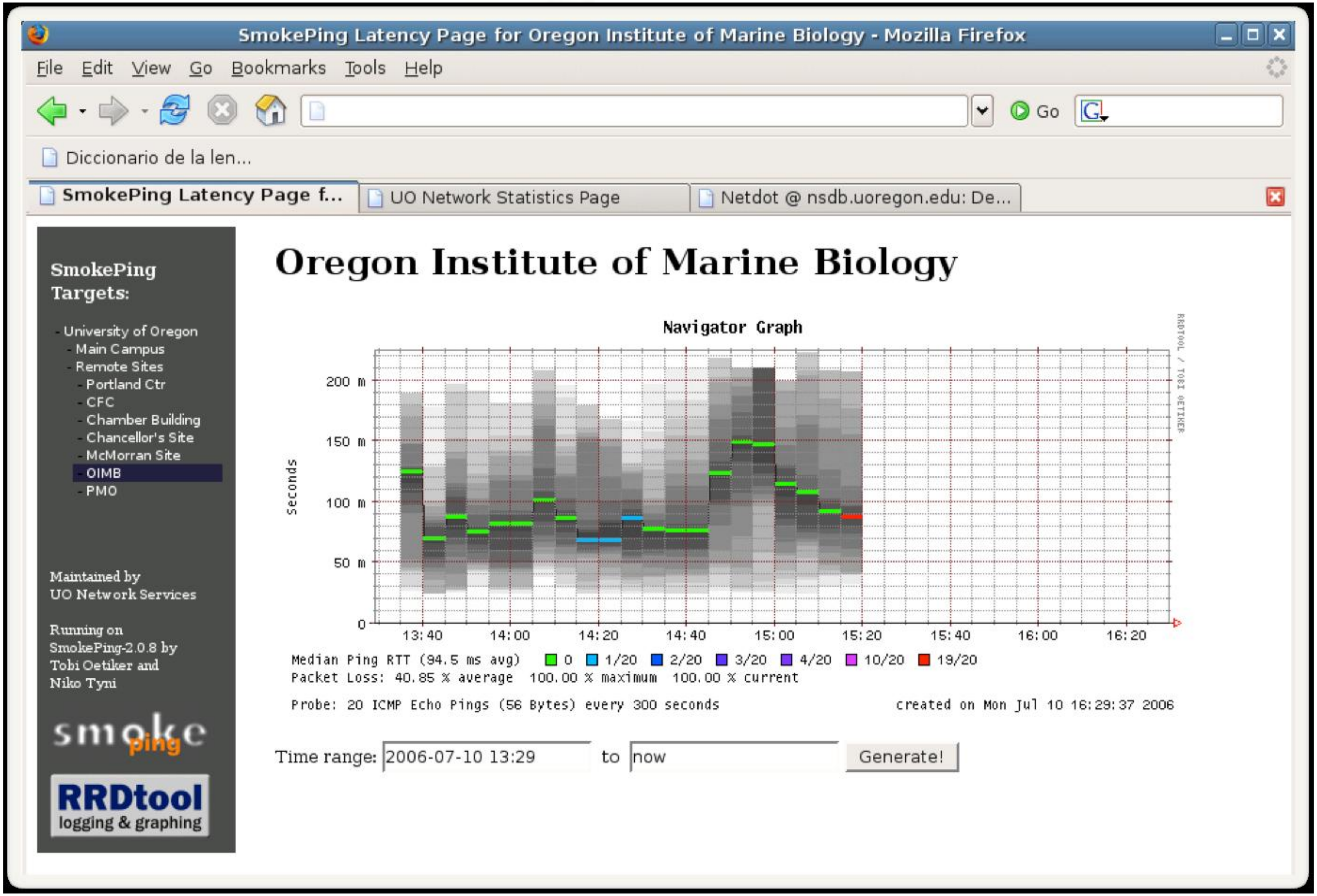
SmokePing - Introduction

- Based on RRDTool (the same author)
- Measures latency and can measure performance and status of services such as HTTP, DNS, SMTP, SSH, LDAP, etc.
- Define ranges on statistics and generate alarms.
- Written in Perl for portability
- Easy to install harder to configure.

SmokePing – “Marketing”

- SmokePing keeps track of your network latency:
- Best of breed latency visualization.
- Interactive graph explorer.
- Wide range of latency measurement 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 written by Tobi Oetiker, the creator of MRTG and RRDtool

Sample Screenshot



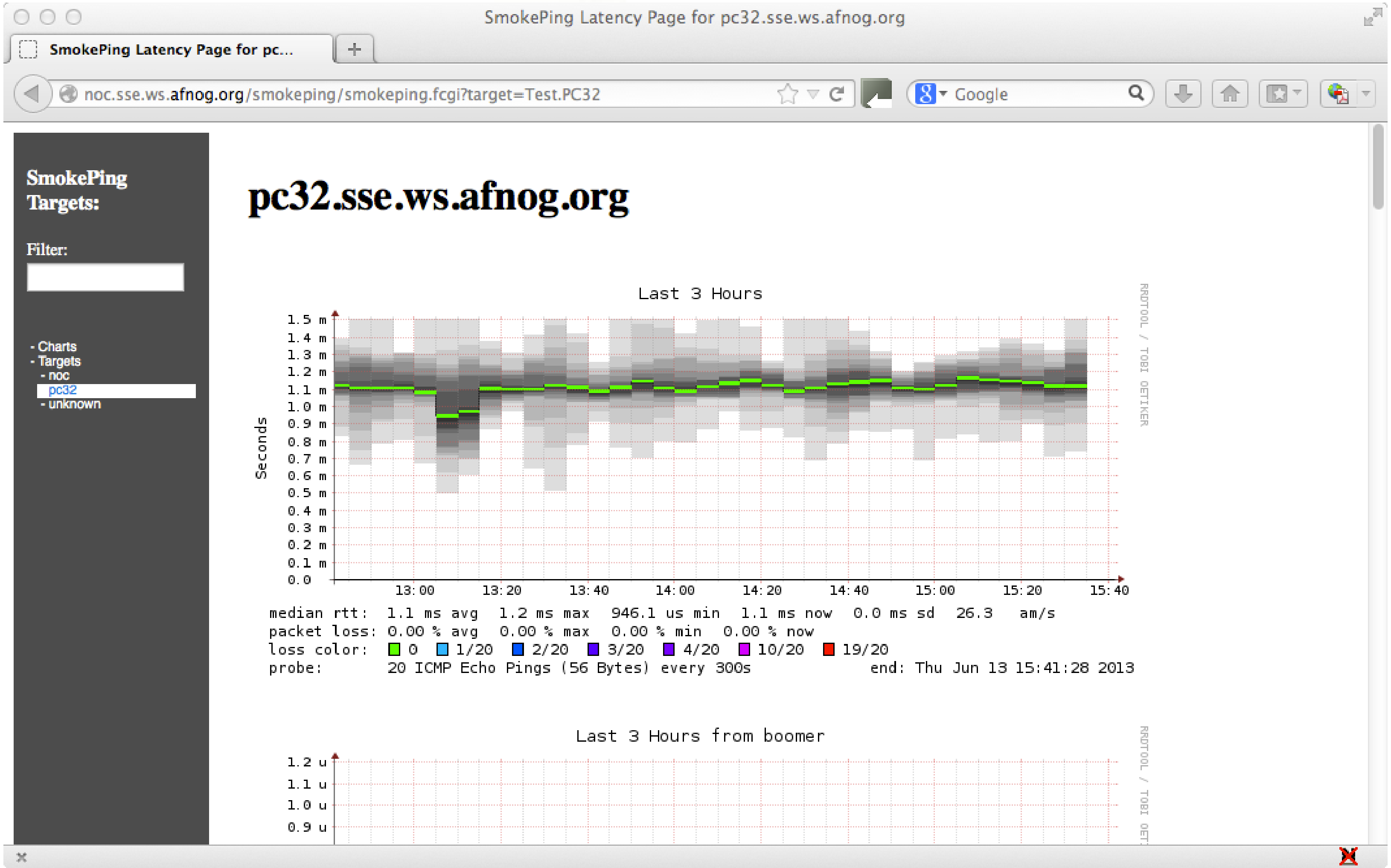
```
Median Ping RTT (94.5 ms avg)  🟩 0  🟦 1/20  🟦 2/20  🟪 3/20  🟪 4/20  🟪 10/20  🟥 19/20
Packet Loss: 40.85 % average   100.00 % maximum   100.00 % current

Probe: 20 ICMP Echo Pings (56 Bytes) every 300 seconds                 created on Mon Jul 10 16:29:37 2006
```

Time range: 2006-07-10 13:29 to now

Reading Smokeping Graphs

- **Smokeping sends multiples tests (pings), makes note of RTT, orders these and selects the median.**
- **The different values of RTT are shown graphically as lighter and darker shades of grey (the “smoke”). This conveys the idea of variable round trip times or *jitter.***
- **The number of lost packets (if any) changes the color of the horizontal line across the graph.**

Reading Smokeping Graphs



SmokePing Latency Page for pc32.sse.ws.afnog.org

noc.sse.ws.afnog.org/smokeping/smokeping.fcgi?target=Test.PC32

SmokePing Targets:

Filter:

- Charts
- Targets
  - noc
  - pc32
  - unknown

pc32.sse.ws.afnog.org

Last 3 Hours

```
median rtt:   1.1 ms avg   1.2 ms max   946.1 us min   1.1 ms now   0.0 ms sd   26.3   am/s
packet loss:  0.00 % avg   0.00 % 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 Jun 13 15:41:28 2013
```

Last 3 Hours from boomer

Dependencies

RRDtool	http://oss.oetiker.ch/rrdtool/
Fping	http://www.fping.com/
Echoping	http://echoping.sourceforge.net/
Apache	http://httpd.apache.org/
Perl	http://www.perl.org/
FCGI	http://www.fastcgi.com/drupal/
speedyCGI	http://www.daemoninc.com/SpeedyCGI/

SmokePing – Installation

- FreeBSD ports:

```
# cd /usr/ports/net-mgmt/smokeping
# make all install clean
```

- Configuration file:

```
/usr/local/etc/smokeping/config
```

- Change Smokeping’s appearance:

```
/usr/local/etc/smokeping/basepage.html
```

- Restart the service:

```
/usr/local/etc/smokeping restart
/usr/local/etc/smokeping reload
```

SmokePing – config file

- Config file is set out in the following sections:
  - General
  - Database
  - Presentation
  - Probes
  - Slaves
  - Targets

- Generally most time is spent configuring Targets, Probes and Alerts

SmokePing config - General

```
*** General ***

owner    = Peter Random
contact  = noc@localhost
mailhost = localhost
sendmail = /usr/sbin/sendmail
# NOTE: do not put the Image Cache below cgi-bin
# since all files under cgi-bin will be executed ... this is not
# good for images.
imgcache = /usr/local/smokeping/htdocs/img
imgurl   = img
datadir  = /usr/local/var/smokeping
piddir  = /usr/local/var/smokeping
cgiurl   = http://pc32.sse.ws.afnog.org/smokeping.cgi
smokemail = /usr/local/etc/smokeping/smokemail
tmail = /usr/local/etc/smokeping/tmail
# specify this to get syslog logging
syslogfacility = local0
# each probe is now run in its own process
# disable this to revert to the old behaviour
# concurrentprobes = no
```

SmokePing config - Alerts

- Very flexible and you can create your own type of alert.
- Send alerts to ticket queues (RT using rt-mailgate, for instance)
- Somewhat complex to understand. Read the Alerts section of the Smokeping on-line configuration documentation:
  http://oss.oetiker.ch/smokeping/doc/smokeping_config.en.html

```
*** Alerts ***

to = noc@localhost
from = smoke-alert@localhost

+someloss
type = loss
# in percent
pattern = >0%,*12*,>0%,*12*,>0%
comment = loss 3 times  in a row
```

SmokePing config - Database

- Defines how RRDtool will save data over time in Round Robin Archives (RRAs)
- By default each step is 300 seconds (5 minutes).
- You cannot trivially change the step setting once data has been collected.
- Details on each column in the Database section of the Smokeping on-line configuration documentation:
  http://oss.oetiker.ch/smokeping/doc/smokeping_config.en.html

```
*** Database ***

step     = 300
pings    = 20

# consfn mrhb steps total

AVERAGE  0.5   1  1008
AVERAGE  0.5  12  4320
    MIN  0.5  12  4320
    MAX  0.5  12  4320
AVERAGE  0.5 144   720
    MAX  0.5 144   720
    MIN  0.5 144   720
```

consfn: Consolidation function

mrhb: Percent of consolidated steps that must be known to warrant an entry.

steps: How many steps to consolidate for each entry in the RRA.

total: Total number of rows to keep in the RRA. Use rows and steps to determine time data will be saved.

12 steps = 12 x 300 sec = 1 hour
4320 rows = 4320 hours = 180 days

SmokePing config - Presentation

- If you wish to customize Smokeping’s look and feel you can edit the file /etc/smokeping/basepage.html
- To change how Smokeping presents graphs you can edit this section.

```
*** Presentation ***

template = /usr/local/etc/smokeping/basepage.html

+ charts

menu = Charts
title = The most interesting destinations

++ stddev
sorter = StdDev(entries=>4)
title = Top Standard Deviation
menu = Std Deviation
format = Standard Deviation %f

++ max
sorter = Max(entries=>5)
title = Top Max Roundtrip Time
menu = by Max
format = Max Roundtrip Time %f seconds
```

SmokePing config - Probes

- Smokeping is installed with a number of additional probes. They must, however, be specified here – including their default behaviors.

```
*** Probes ***

+ FPing
binary = /usr/local/sbin/fping

+ DNS
binary = /usr/bin/dig
lookup = afnog.org
pings = 5
step = 180

+ EchoPingHttp
binary = /usr/bin/echoping
ignore_cache = yes
pings = 5
url = /

+ EchoPingHttps
binary = /usr/bin/echoping
pings = 5
url = /

+ EchoPingSmtp
binary = /usr/bin/echoping
forks = 5
```

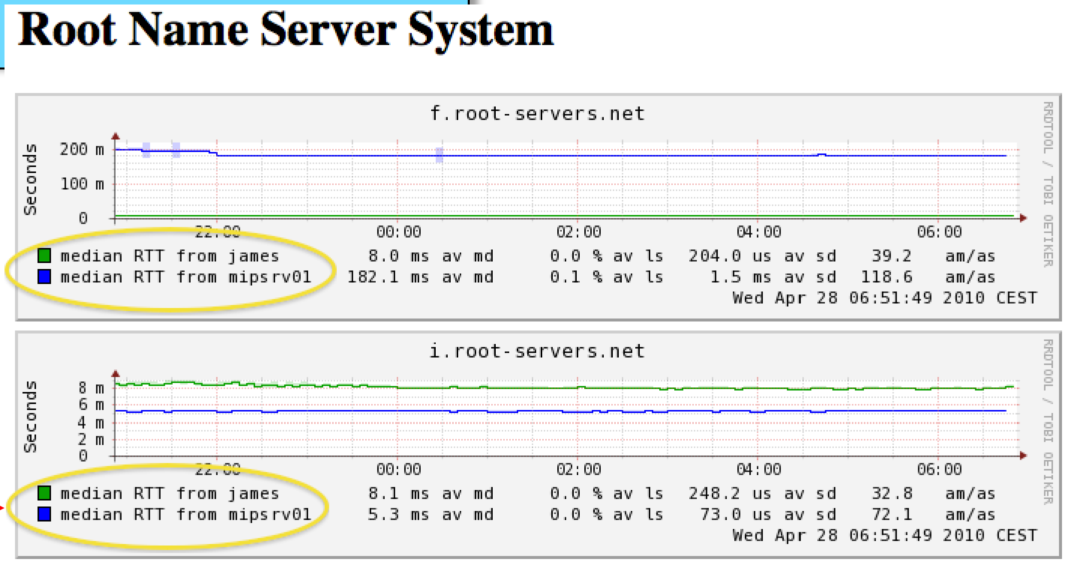
Use the DNS probe to verify that your services are available and responding as expected.

We use ”afnog.org” as a sample hostname to lookup, to verify that the DNS works.

SmokePing config - Slaves

- Smokeping slave servers allow for multi-viewpoint monitoring and graphing of the same services, machines or links. Details here:
  http://oss.oetiker.ch/smokeping/doc/smokeping_master_slave.en.html

```
*** Slaves ***
secrets=/usr/local/etc/smokeping/smokeping_secrets

+boomer
display_name=boomer
color=0000ff

+slave2
display_name=another
color=00ff00
```



Root Name Server System

```
f.root-servers.net
🟩 median RTT from james       8.0 ms av md   0.0 % av ls   204.0 us av sd    39.2   am/as
🟦 median RTT from mipsrv01  182.1 ms av md   0.1 % av ls     1.5 ms av sd   118.6   am/as
                                                      Wed Apr 28 06:51:49 2010 CEST
```

```
i.root-servers.net
🟩 median RTT from james       8.1 ms av md   0.0 % av ls   248.2 us av sd    32.8   am/as
🟦 median RTT from mipsrv01    5.3 ms av md   0.0 % av ls    73.0 us av sd    72.1   am/as
                                                      Wed Apr 28 06:51:49 2010 CEST
```

That is, you can externally monitor your network!

SmokePing config - Targets

- Where we spend most of our time configuring Smokeping.
- Web menu hierarchy defined by "+", "++", etc.
- Each new *probe statement* resets the default probe in use.
- Probes have defaults set in the Probes config file. These can be overridden in Targets section.

```
*** Targets ***
probe = FPing
menu = Top
title = Network Latency Grapher

+ UO
menu = University of Oregon
title = UO webserver
host = www.uoregon.edu

+ NSRC
menu = NSRC
title = Network Startup Resource
Center
host = www.nsrc.org

++ HTTP
menu = HTTP
probe = EchoPingHttp

+++ www
menu = NSRC web
host = www.nsrc.org
++ DNS
menu = DNS
probe = DNS
+++ dns
menu = NSRC DNS
host = www.nsrc.org
```

SmokePing – Default Probe

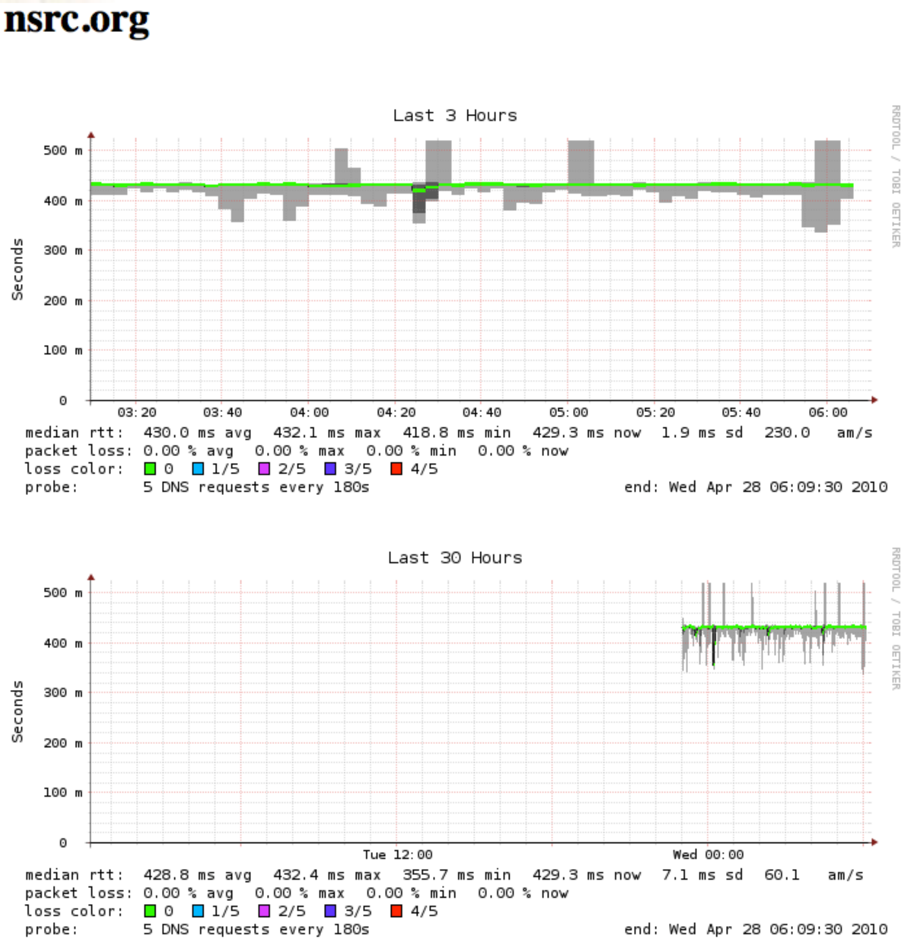
- Probing for delay and jitter (ping)
- Performance and availability probe of a server.
- Entry belongs in the Targets section of the config file:

```
+++ LocalMachine
menu = localhost
title = Our Local Machine
alerts = someloss
host = localhost
```

SmokePing – DNS Check

- Entry belongs in the Targets section of the config file:

```
++ DNS
probe = DNS
menu = External DNS Check
title = DNS Latency
+++ nsrc
host = nsrc.org
```



nsrc.org

```
median rtt:  430.0 ms avg  432.1 ms max  418.8 ms min  429.3 ms now  1.9 ms sd  230.0   am/s
packet loss: 0.00 % avg  0.00 % max  0.00 % min  0.00 % now
loss color:  🟩 0  🟦 1/5  🟪 2/5  🟪 3/5  🟥 4/5
probe:       5 DNS requests every 180s                              end: Wed Apr 28 06:09:30 2010
```

```
median rtt:  428.8 ms avg  432.4 ms max  355.7 ms min  429.3 ms now  7.1 ms sd  60.1   am/s
packet loss: 0.00 % avg  0.00 % max  0.00 % min  0.00 % now
loss color:  🟩 0  🟦 1/5  🟪 2/5  🟪 3/5  🟥 4/5
probe:       5 DNS requests every 180s                              end: Wed Apr 28 06:09:30 2010
```

SmokePing – Other Probes

- More information available here:
  - http://oss.oetiker.ch/smokeping/probe/index.en.html
- A few more probes…

- DNS
- HTTP(S)
- LDAP
- Whois
- SMTP

- CiscoRTTMonDNS
- CiscoRTTMonTcpCon
- Tacacs
- WebProxyFilter - Etc.

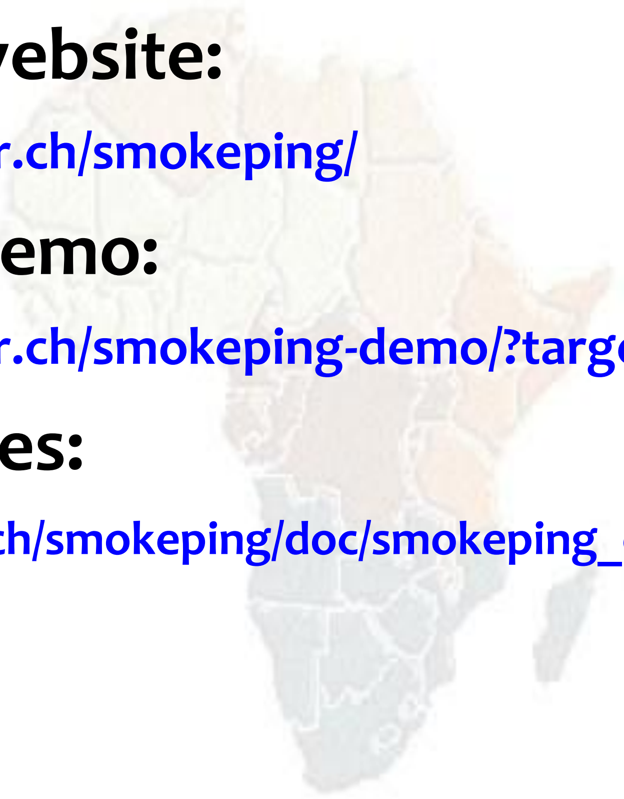
-WWW-Cache

- Radius
- IOS
- FPing6
- etc.

SmokePing – Summary

- **Simple but powerful network monitoring**
- **Monitor machines, services and link health**
- **Distributed instances for external views often a paid-for service**
- **Easy to configure and customize, but very extensible.**
- **Can be used with Ticketing Systems to automate alerts**
- **Very small disk and CPU footprint**

References



- **Smokeping website:**

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

- **Smokeping Demo:**

  http://oss.oetiker.ch/smokeping-demo/?target=Customers.OP

- **Good examples:**

  http://oss.oetiker.ch/smokeping/doc/smokeping_examples.en.html