
# Baseline, Monitor, Detect, Analyze, Respond, & Recover

Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnauld 2009 Santiago, Chile

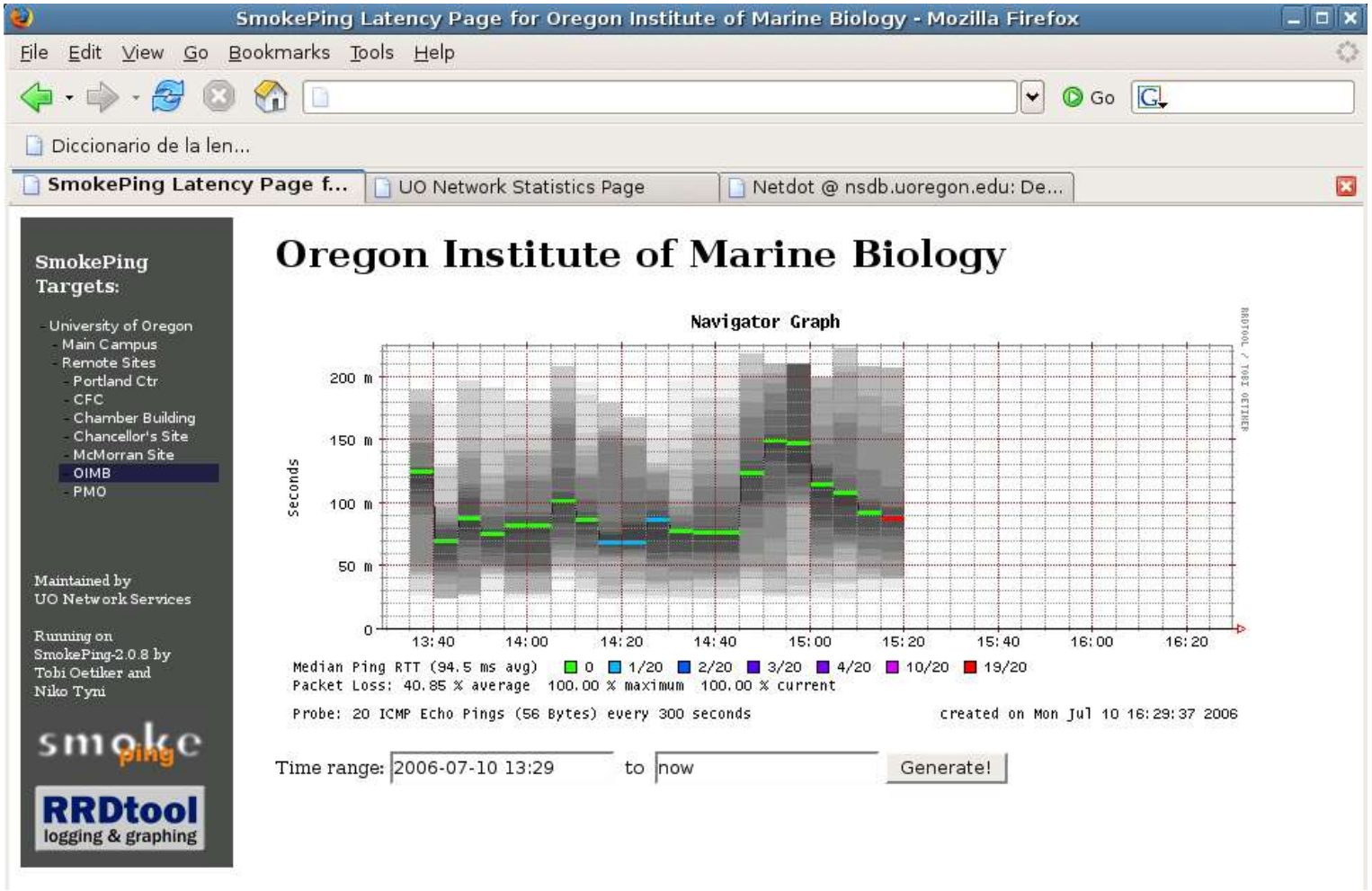

# Introduction

- Based on RRDTool (the same author)
- Measures ICMP delay and can measure status of services such as HTTP, DNS, SMTP, SSH, LDAP, etc.
- Allows you to define ranges on statistics and generate alarms.
- Written in Perl for portability
- Relatively easy to install. In Debian it's very simple.

# How to Read Smokeping Graphs

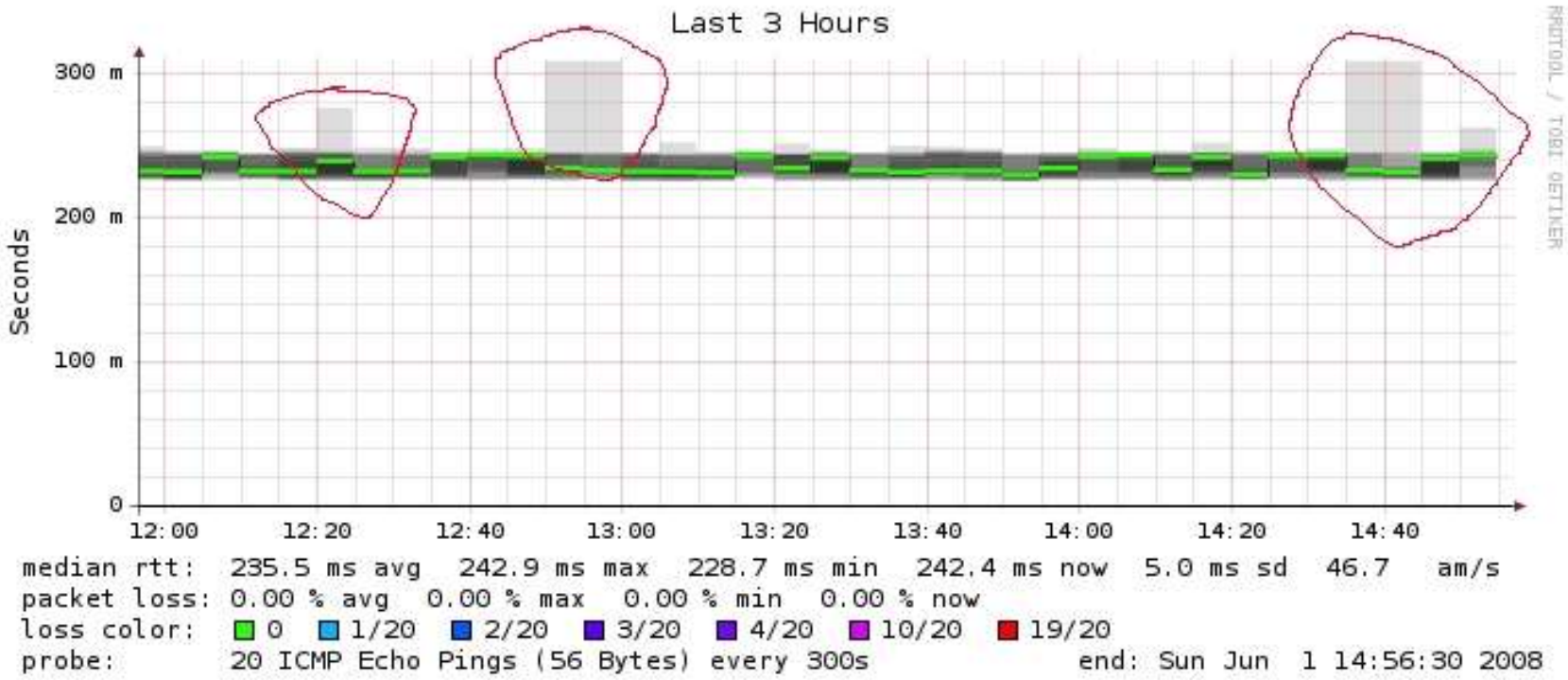
- Smokeping sends multiples tests (pings), makes note of RTT, orders these and selects the median.
- The different values of RTT are shown graphically as lighter and darkers shades of grey (the “smoke”). This conveys the idea of variable round trip times or *jitter*.
- The number of lost packets (if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

# The “Smoke” and the “Pings”



# Another Examples

## African Network Operators Group



# Requirements

- The following packages are needed or recommended:
  - rrdtool http://oss.oetiker.ch/rrdtool/
  - fping http://www.fping.com/
  - echoping http://echoping.sourceforge.net/
  - speedyCGI http://www.daemoninc.com/SpeedyCGI/
  - Apache http://httpd.apache.org
  - Perl

# Smokeping: Installation

- `apt-get install smokeping`
- Configure **/etc/smokeping/config.d/***
- Change Smokeping's appearance here:
  - **/etc/smokeping/basepage.html**
- Restart the service:
  - **/etc/init.d/smokeping restart**
  - **/etc/init.d/smokepring reload**

# Smokeping: Installation

- You will find Smokeping running here:

- http://192.168.10x.30/cgi-bin/smokeping.cgi

# Configuration

- The Smokeping configuration files are:
  /etc/smokeping/config.d/*
- They contain:
  - The locations of directories and components
  - Configuration of the probes used
  - Destination nodes and the format of the hierarchical Smokeping menu.
    - Each '+' adds a level to the hierarchy
- In addition */etc/smokeping/basepage.html* allows you to change the look and feel of the initial Smokeping web page.

# Configuration Files

- The listing of files in /etc/smokeping/config.d:
- **Alerts**: Define patterns of response probes to generate an alert – i.e., send an email.
- **Database**: How many seconds to wait and pings to send per probe. Define deviations for graphing.
- ***General***: Local installation owner, syslog facility to use, default URL to view pages, etc.
- **pathnames**: Where programs, configurations and items are kept on the local system.

# Configuration Files cont.

- The listing of files in /etc/smokeping/config.d cont.
- **Presentation**: Define the details of smokeping graphs and charts.
- **Probes**: Available probes and where the binary resides.
- **Slaves**: Define remote smokeping server instances and checks to report back to master server.
- ***Targets***: The file we care the most about. Define all targets you are monitoring, what services to monitor on each target and your display hierarchy on the main smokeping web page.

# Configuration: Alerts

*/etc/smokeping/config.d/Alerts*

```
*** Alerts ***
to = tldadmin@localhost
from = tldadmin@tldX

+bigloss
type = loss
# in percent
pattern = ==0%,==0%,==0%,==0%,>0%,>0%,>0%
comment = suddenly there is packet loss

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

# Configuration: Database

*/etc/smokeping/config.d/Database*

```
*** 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
```

# Configuration: General

*/etc/smokeping/config.d/General*

```
*** General ***

@include /etc/smokeping/config.d/pathnames

# Please edit this to suit your installation
owner    = tldadmin@tldX
contact  = tldadmin@localhost
cgiurl   = http://192.168.10x.30/cgi-
bin/smokeping.cgi
mailhost = localhost
# 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
```

# Configuration: pathnames

*/etc/smokeping/config.d/pathnames*

You generally do not need to edit this file:

```
sendmail = /usr/sbin/sendmail
imgcache = /var/www/smokeping
imgurl   = ../smokeping
datadir  = /var/lib/smokeping
dyndir   = /var/lib/smokeping/__cgi
piddir   = /var/run/smokeping
smokemail = /etc/smokeping/smokemail
tmail    = /etc/smokeping/tmail
precreateperms = 2775
```

# Configuration: Presentation

/etc/smokeping/config.d/Presentation

```
*** Presentation ***

template = /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
```

# Configuration: Probes

/etc/smokeping/config.d/Probes

```
*** Probes ***

+ FPing
binary = /usr/sbin/fping

+ DNS
binary = /usr/bin/dig
lookup = www.uoregon.edu
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
```

# Configuration: Slaves

/etc/smokeping/config.d/Slaves

```
# *** Slaves ***
#
## make sure this is not world-readable!
## secrets=/etc/smokeping/slave-secrets
#
# +slave1
# display_name=slave_name
# color=0000ff
```

# Configuration: Targets

Sample from the file:
*/etc/smokeping/config.d/Targets*

We will look at our classroom Targets configuration file on your NOC.

```
*** Targets ***

probe = FPing

menu = Top
title = Network Latency Grapher

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

+ UTE
menu = UTE
title = Universidad Tecnologica
Equinoccial

++ HTTP
menu = HTTP
probe = EchoPingHttp

+++ www
menu = UTE web
host = www.ute.edu.ec

++ DNS
menu = DNS
probe = DNS

+++ dns
menu = UTE DNS
host = www.ute.edu.ec
```

# Default Probe: Ping

- **Probing for delay and jitter (ping)**
- **Performance and availability probe of a server:**

**Latency**

```
+++ LocalMachine
menu = NOC
title = The NOC@netmanage
host = localhost
alerts = startloss,someloss,bigloss,rttdetect,hostdown
```

# Another Type of Probe

- **Performance and Availability**

```
++ MyWebServer
menu = Web server
title = webserver for aftld.org
probe = EchoPingHttp
host = www.aftld.org
port = 80
url = http://www.aftld.org/
```

# More Types of Probes

- **More information available here:**
  `http://oss.oetiker.ch/smokeping/probe/index.en.html`

- **A few more probes...**
  - DNS - CiscoRTTMonDNS - Radius
  - HTTP(S) - CiscoRTTMonTcpCon - IOS
  - LDAP - Tacacs - FPing6
  - Whois - WebProxyFilter - Etc.
  - SMTP - WWW-Cache

# Exercises

- Configure your machine so that it monitors localhost, as well as tldX-rtr (192.168.10x.1) and the ISP-rtr (192.168.96.1)
- The idea is:
  - Add entries in /etc/smokeping/config.d/Targets for each of the above hosts.
  - Use ping (the default probe) for this

# More Exercises

- If you finish the previous exercises, then you can always add the other TLDs' routers and servers.
- You can add checks for machines outside of our network.
  - Maybe add an entry for some faraway site (your own DNS servers back home ?)
- Other possibilities include:
  - Email alerts send when certain conditions are met.
  - Adding a group of machines by a single type of probe in a single graph – i.e. aggregate result graphs. Very useful for quickly reviewing a group of machines and a single service.

# References

- Smokeping website:
  http://oss.oetiker.ch/smokeping/
- Good examples:

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

# Questions ?