Network Monitoring and Management

Tutorial: APNIC 34

These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (http://creativecommons.org/licenses/by-nc/3.0/) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Demonstration of Tools

- SNMP
- Cacti
- Logging (syslog-ng / swatch)
- Nagios
- RANCID
- Smokeping
- NetFlow / NfSen
- Netdot

Introduction

- 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.

Plugins

Plugins are used to verify services and devices:

–Nagios architecture is simple enough that writing new plugins is fairly easy in the language of your choice.

–There are ***many, many*** plugins available (thousands).

✓http://exchange.nagios.org/

✓http://nagiosplugins.org/

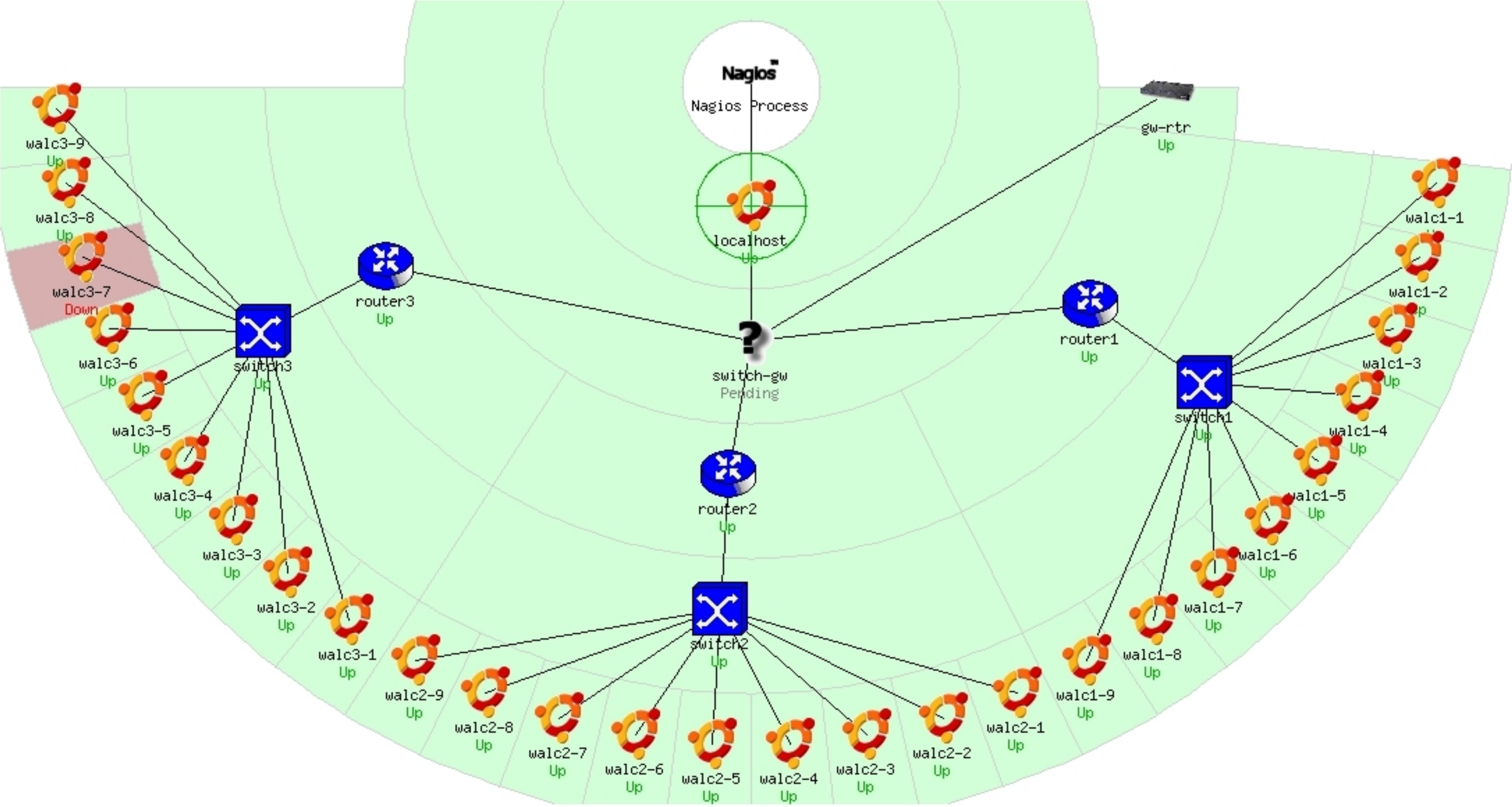
Features

- Configuration done in text files, based on templates.
- Nagios reads its configuration from a directory. You determine how to divide your configuration files.
- Uses parallel checking and forking for scalability

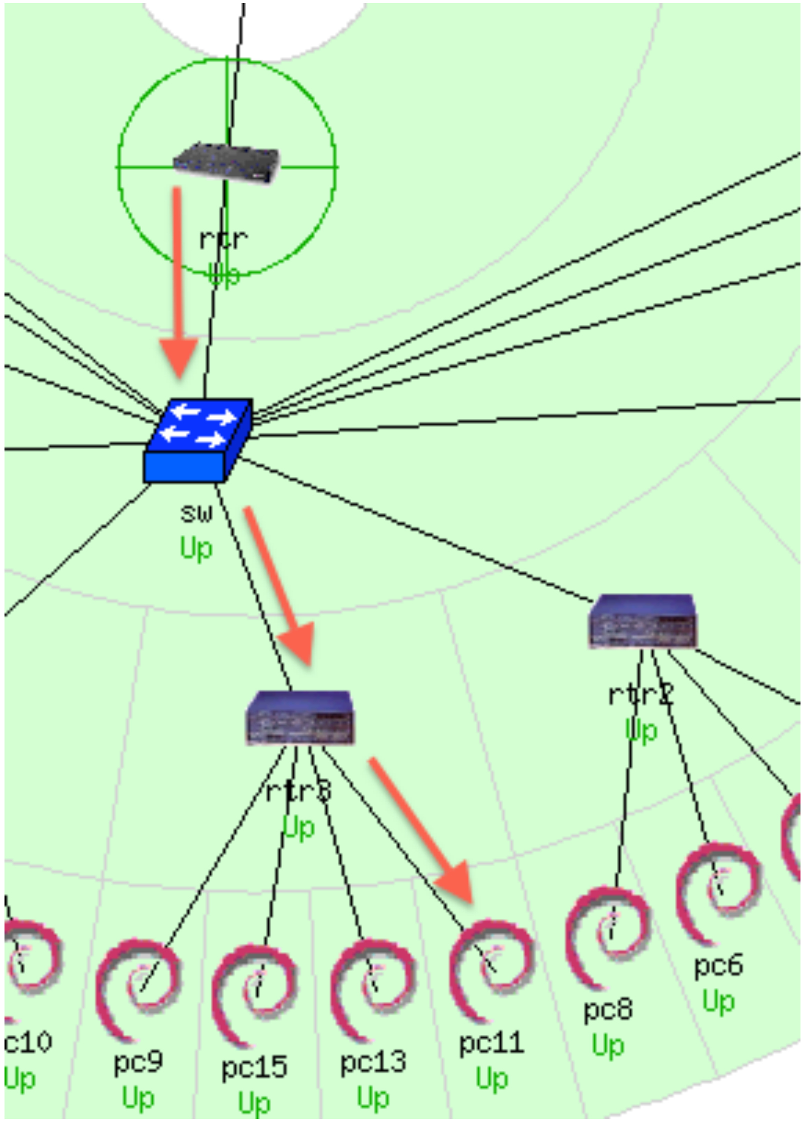
Features cont.

- Utilizes topology to determine dependencies.
    - Differentiates between what is *down* vs. what is *unreachable*. Avoids running unnecessary checks and sending redundant alarms
- Allows you to define how to send notifications based on combinations of:
    - Contacts and lists of contacts
    - Devices and groups of devices
    - Services and groups of services
    - Defined hours by persons or groups.
    - The state of a service.

Network viewpoint



Parents and configuration



RTR

```
define host {
    use             generic-host
    host_name       rtr
    alias           Gateway Router
    address         10.10.0.254     }
```

SW

```
define host {
    use             generic-host
    host_name       sw
    alias           Backbone Switch
    address         10.10.0.253
    parents         rtr     }
```

RTR3

```
define host {
    use             generic-host
    host_name       rtr3
    alias           router 3
    address         10.10.3.254
    parents         sw      }
```

PC11…

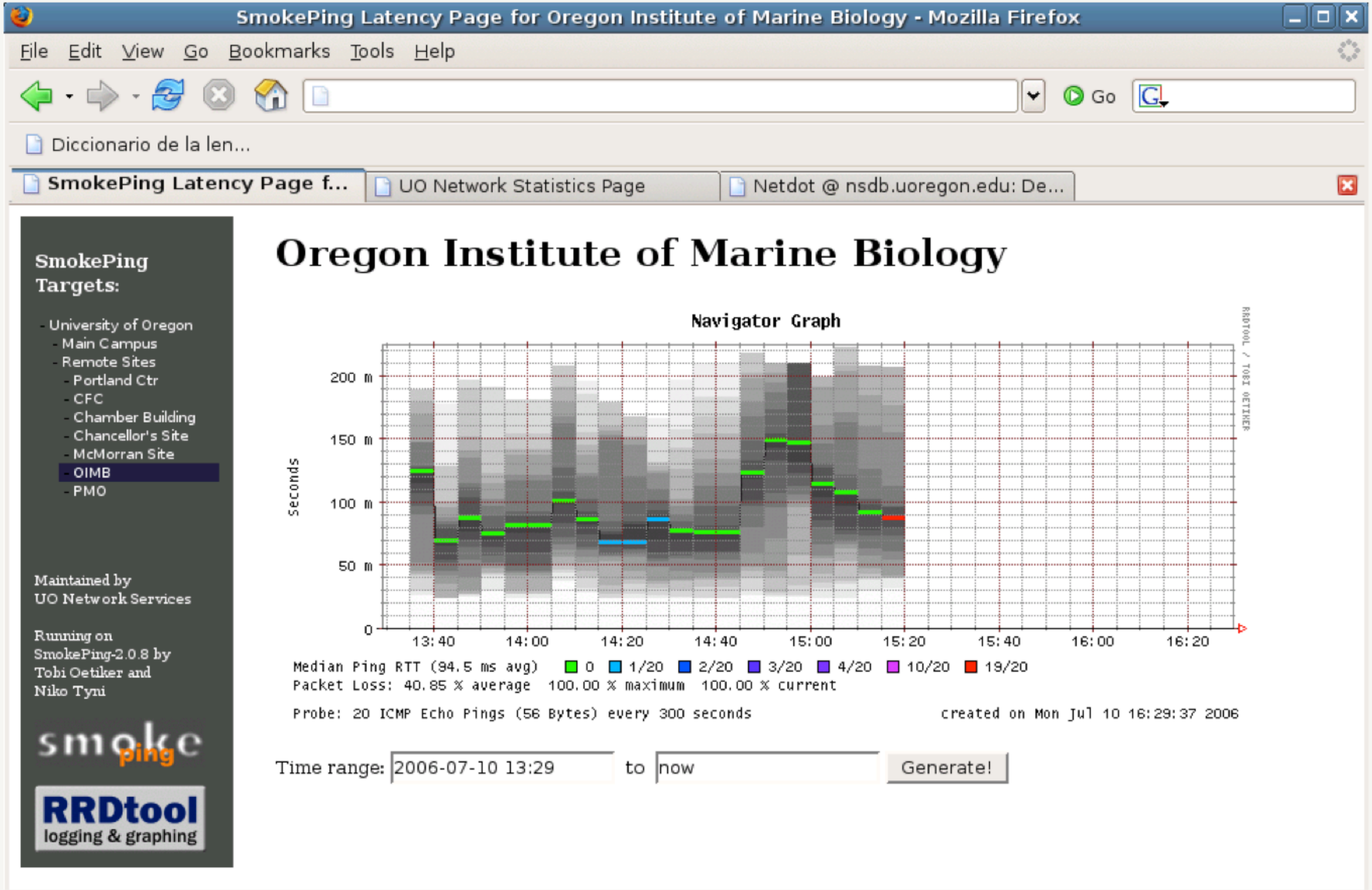
Demonstration of Tools

- SNMP
- Cacti
- Logging (syslog-ng / swatch)
- Nagios
- RANCID
- Smokeping
- NetFlow / NfSen
- Netdot

Introduction

- Based on RRDTool (the same author)
- Measures ICMP delay and can measure 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.

The “Smoke” and the “Pings”


SmokePing Latency Page for Oregon Institute of Marine Biology - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Diccionario de la len...
SmokePing Latency Page f...
UO Network Statistics Page
Netdot @ nsdb.uoregon.edu: De...

SmokePing Targets:

- University of Oregon
  - Main Campus
  - Remote Sites
    - Portland Ctr
    - CFC
    - Chamber Building
    - Chancellor's Site
    - McMorran Site
    - OIMB
    - PMO

Maintained by
UO Network Services

Running on
SmokePing-2.0.8 by
Tobi Oetiker and
Niko Tyni

smoke ping
RRDtool logging & graphing

Oregon Institute of Marine Biology

Navigator Graph
Seconds
200 m
150 m
100 m
50 m
0
13:40
14:00
14:20
14:40
15:00
15:20
15:40
16:00
16:20
RRDTOOL / TOBI OETIKER

```
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 Generate!

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 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.

Demonstration of Tools

- SNMP
- Cacti
- Logging (syslog-ng / swatch)
- Nagios
- RANCID
- Smokeping
- NetFlow / NfSen
- Netdot

Network Flows (NetFlow)

- Packets or frames that have a common attribute.
- Creation and expiration policy – what conditions start and stop a flow.
- Counters – packets, bytes, time.
- Routing information – AS, network mask, interfaces.

Network Flows

- Unidirectional or bidirectional.
- Bidirectional flows can contain other information such as round trip time, TCP behavior.
- Application flows look past the headers to classify packets by their contents.
- Aggregated flows – flows of flows.

Working with Flows

- Generate the flows from device (usually a router)
- Export flows from the device to collector
  - Configure version of flows
  - Sampling rates
- Collect the flows
  - Tools to Collect Flows - Flow-tools
  - NfSen
- Analyze them
  - More tools available, can write your own

What is NfSen

- Is a graphical front end to nfdump
- NfDump tools collect and process netflow data on the command line
- NfSEN allows you to:
  - 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.
  - Write your own plugins to process netflow data on a regular interval.

Demonstration of Tools

- SNMP
- Cacti
- Logging (syslog-ng / swatch)
- Nagios
- RANCID
- Smokeping
- NetFlow / NfSen
- Netdot

Problems with documentation

In most cases:

- Lack of clear procedures and methods
- Dispersion
- Lack of structure
- Lack of correlation
- Lack of tools… or, too many tools
- Lack of time and human resources

Netdot: {net.} NETwork DOcumentation Tool

- Started in 2002. Required by the University of Oregon Network Services and NERO (http://www.nero.net)
- Nothing equivalent available as Open Source
- Started as something much simpler
- Quickly it became apparent that centralizing and correlating information was critical:
  - Topology
  - Cable plant
  - IP and Mac addresses
  - DNS, DHCP, etc.

Netdot: Design goals

- Utilize components (don’t reinvent the wheel)
  - There are Open Source packages that help to resolve many Network Management problems.
- Independent of the RDBMS using abstraction (http://www.masonhq.com)
  - MySQL, Postgres, etc.
- Use of Object Relations Mapper tools (ORM)
- Minimize the number of programming languages.
  - Perl and Javascript
- Low impact graphical interface.

{net.} NETwork DOcumentation Tool

Include functionality of other network documenation tools such as IPplan and Netdisco.

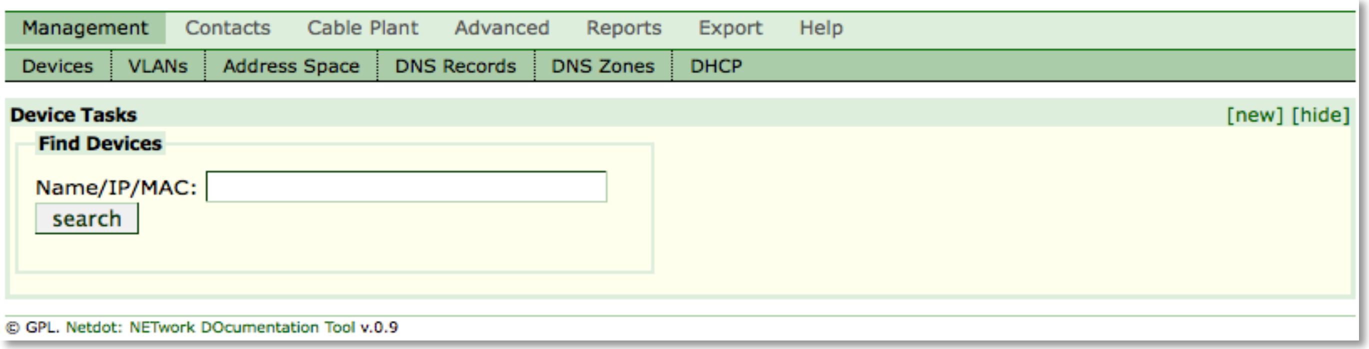
Core functionality includes:

- Discovery of network interfaces via SNMP
- Layer 2 topology discovery and graphics using:
  - CDP/LLDP
  - Spanning Tree protocol
  - Switches forwarding tables
  - Router point-to-point subnets
- IPv4 and IPv6 address management (IPAM)
  - Address space visualization
  - DNS and DHCP configuration managment
  - IP and Mac address correlation

{net.} NETwork DOcumentation Tool

Functionality cont.

- Cable plants (sites, fibre, copper, closes, circuits)
- Contacts (departments, providers, vendors, etc.)
- Export of data for various tools (Nagios, Sysmon, RANCID, Cacti, etc.)
  - For example, automate Cacti configuration
  - I.E., how to automate node creation in Cacti
- User access-level: admin, operator, user
- Ability to draw pretty pictures of your network.



Device Tasks

Find Devices

Name/IP/MAC:

© GPL. Netdot: NETwork DOcumentation Tool v.0.9

Questions?

?