Network Monitoring and Management

Tutorial: SANOG 2015

What we'll show and talk about

1. Network Monitoring and Management overview
   - Challenges, concepts, motivations
2. Presentation of protocols, services, tools & techniques
   - **SNMP & Cacti:** Data collection and graphing
   - **Syslog & syslog-ng + Swatch:** Remote logging, log collection, parsing and alerting
   - **Nagios:** System & Service availability, trend reporting, alarm
   - **RANCID:** Configuration management
   - **SmokePing:** Latency monitoring
   - **NetFlow + NFSen:** Traffic sampling, collection and graphing
   - **Netdot:** Network discovery, inventory management, IP address management & provisioning of the above tools

Different Types of Monitoring

Interactive diagnostics vs automated

- Interactive: ping, traceroute, tcpdump, …
- Usually as an initial investigation of the cause of a problem
- “Drill down”

Active vs passive

- Active, or probing, using ICMP, TCP/UDP, SNMP
- Passive using syslog, netflow, snmp
- Both are used
- Automated monitoring of these resources, to implement alerting & automatic creation of service tickets

Network Management Details

We Monitor

- **System & Services**
  - Available, reachable
- **Resources**
  - Expansion planning, maintain availability
- **Performance**
  - Round-trip-time, throughput
- **Changes and configurations**
  - Documentation, revision control, logging

Network Management Details

We Keep Track Of

- **Statistics**
  - For purposes of accounting and metering
  - Capacity planning
- **Faults**
  - Troubleshooting issues and tracking their history
  - Equipment failure
  - Abuse / Attacks
  - Misconfiguration

- Ticketing systems are good at this
- Help Desks are a useful to critical component

Expectations

A network in operation needs to be monitored in order to:

- Deliver projected SLAs (Service Level Agreements)
- SLAs depend on policy
  - What does your management expect?
  - What do your users expect?
  - What do your customers expect?
  - What does the rest of the Internet expect?
- What's good enough? 99.999% Uptime?
  - There's no such thing as 100% uptime (as we'll see) →

“Uptime” Expectations

What does it take to deliver 99.9 % uptime?

30.5 days x 24 hours = 732 hours a month

(732– (732 x .999)) x 60 = 44 minutes

only 44 minutes of downtime a month!

Need to shutdown 1 hour / week?

(732 – 4) / 732x 100 = 99.4 %

Remember to take planned maintenance into account in your calculations, and inform your users/customers if they are included/excluded in the SLA

How is availability measured?

In the core? End-to-end? From the Internet?

Baselining

What is normal for your network?

If you've never measured or monitored your network you will need to know things like:

- Typical load on links
- Jitter between endpoints
- Typical percent usage of resources
- Typical amounts of "noise":
  - Network scans
  - Dropped data
  - Reported errors or failures

Why do all this?

Know when to upgrade

- Is your bandwidth usage too high?
- Where is your traffic going?
- Do you need to get a faster line, or more providers?
- Is the equipment too old?

Keep an audit trace of changes

- Record all changes
- Makes it easier to find cause of problems due to upgrades and configuration changes

Keep a history of your network operations

- Using a ticket system lets you keep a history of events.
- Allows you to defend yourself and verify what happened

Why network management?

Accounting

- Track usage of resources
- Bill customers according to usage

Know when you have problems

- Stay ahead of your users! Makes you look good.
- Monitoring software can generate tickets and automatically notify staff of issues.

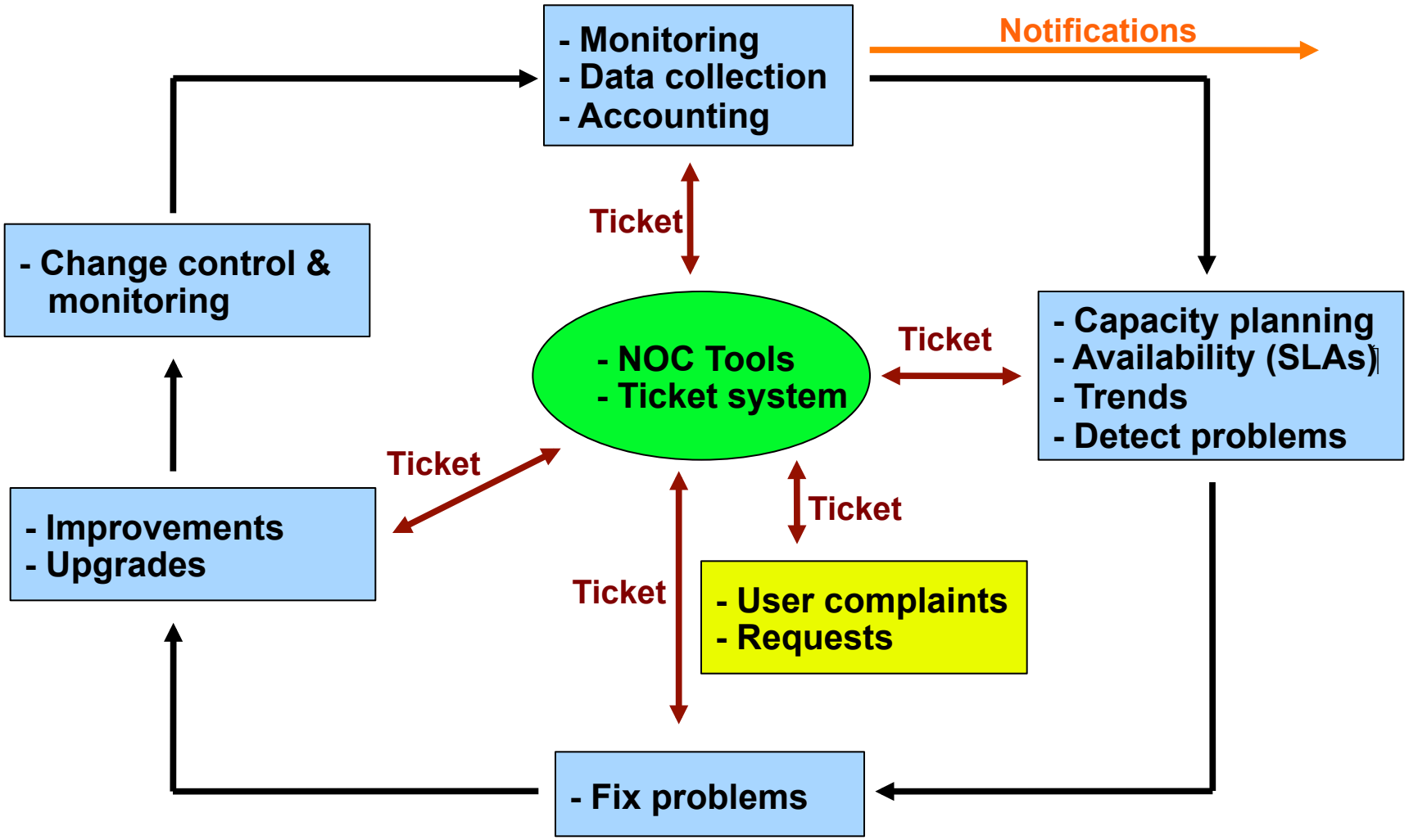
Trends

- All of this information can be used to view trends across your network.
- This is part of baselining, capacity planning and attack detection.

Attack Detection

- Trends and automation allow you to know when you are under attack.
- The tools in use can help you to mitigate attacks:
  - Flows across network interfaces
  - Load on specific servers and/or services
  - Multiple service failures

The big picture



A *few* Open Source solutions…

Performance
- Cricket
- IFPFM
- flowc
- mrtg*
- NetFlow*
- NfSen*
- ntop
- perfSONAR
- pmacct
- rrdtool*
- SmokePing*

Ticketing
- RT*
- Trac*
- Redmine

Change Mgmt
- Mercurial
- Rancid* (routers)
- CVS*
- Subversion*
- git*

Security/NIDS
- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Logging
- swatch*
- syslog/rsyslog*
- tenshi*

Net Management
- Big Brother
- Big Sister
- Cacti*
- Hyperic
- Munin
- Nagios*
- OpenNMS*
- Sysmon
- Zabbix

Documentation
- IPplan
- Netdisco
- Netdot*
- Rack Table

Protocols/Utilities
- SNMP*, Perl, ping

Questions?

?

Demonstration of Tools

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

What is SNMP?

SNMP – Simple Network Management Protocol

- Industry standard, hundreds of tools exist to exploit it
- Present on any decent network equipment

Query – response based: **GET / SET**

- GET is mostly used for monitoring

Tree hierarchy

- Query for ”Object Identifiers” (OIDs)

Concept of MIBs (Management Information Base)

- Standard and vendor-specific (Enterprise)

What is SNMP

Typical queries

- Bytes In/Out on an interface, errors
- CPU load
- Uptime
- Temperature or other vendor specific OIDs

For hosts (servers or workstations)

- Disk space
- Installed software
- Running processes
- ...

Windows and UNIX have SNMP agents

How does it work?

Basic commands

- GET (manager -> agent)
  - Query for a value
- GET-NEXT (manager -> agent)
  - Get next value (list of values for a table)
- GET-RESPONSE (agent -> manager)
  - Response to GET/SET, or error
- SET (manager -> agent)
  - Set a value, or perform action
- TRAP (agent -> manager)
  - Spontaneous notification from equipment (line down, temperature above threshold, ...)

Demonstration of Tools

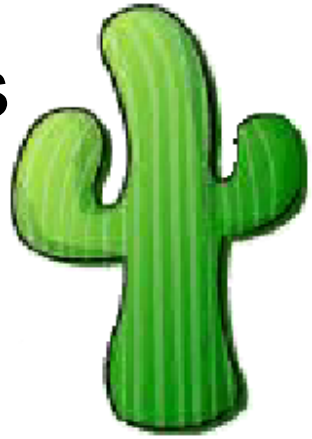
- SNMP
- Cacti
- Logging (syslog-ng / swatch)
- Nagios
- RANCID
- Smokeping
- NetFlow / NfSen
- Netdot

Introduction: Cacti

- 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.
- You can find Cacti here:
  http://www.cacti.net/

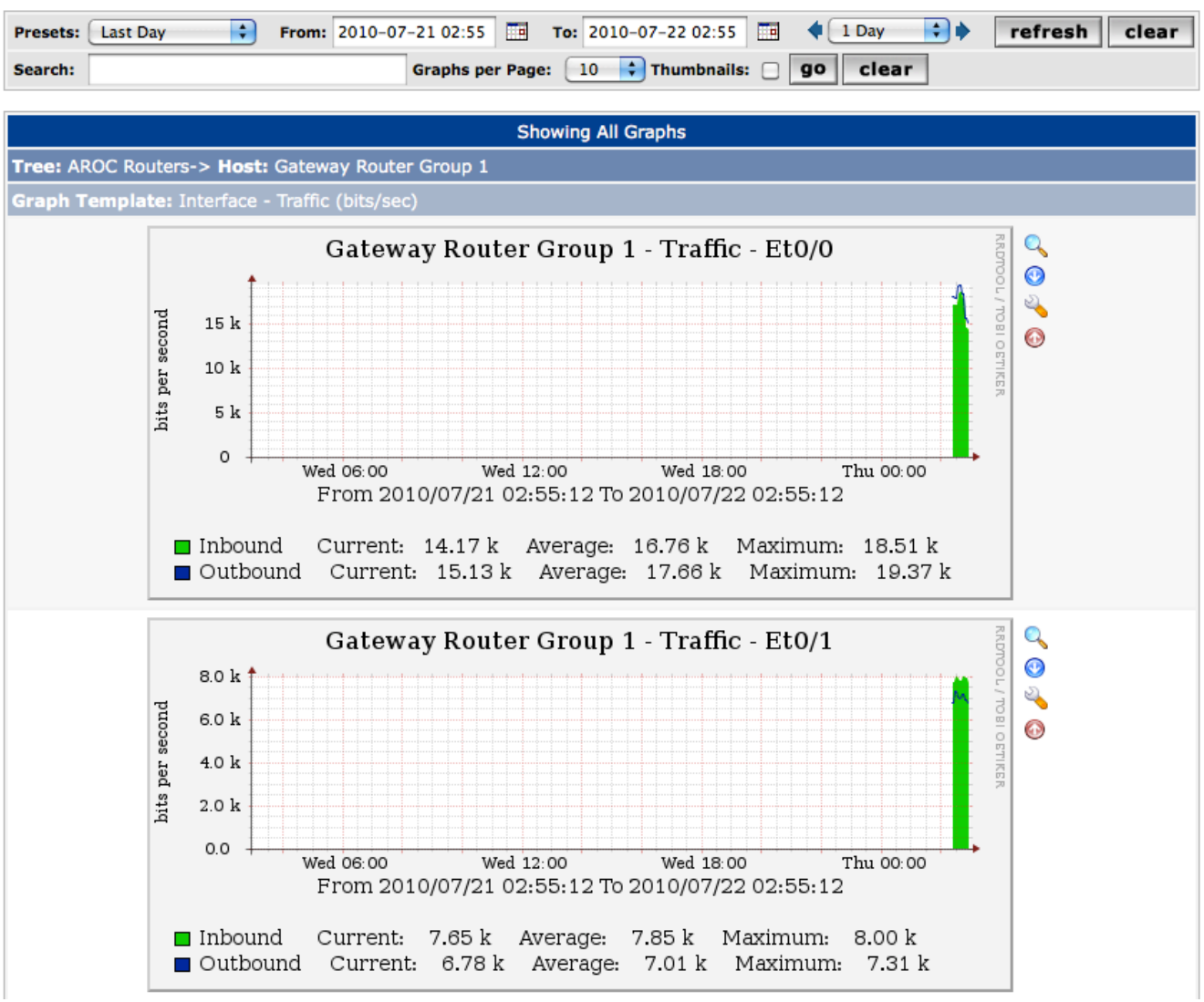
Introduction: Cacti

Cacti: Uses RRDtool, PHP and stores data in MySQL. It supports the use of SNMP and graphics with MRTG.

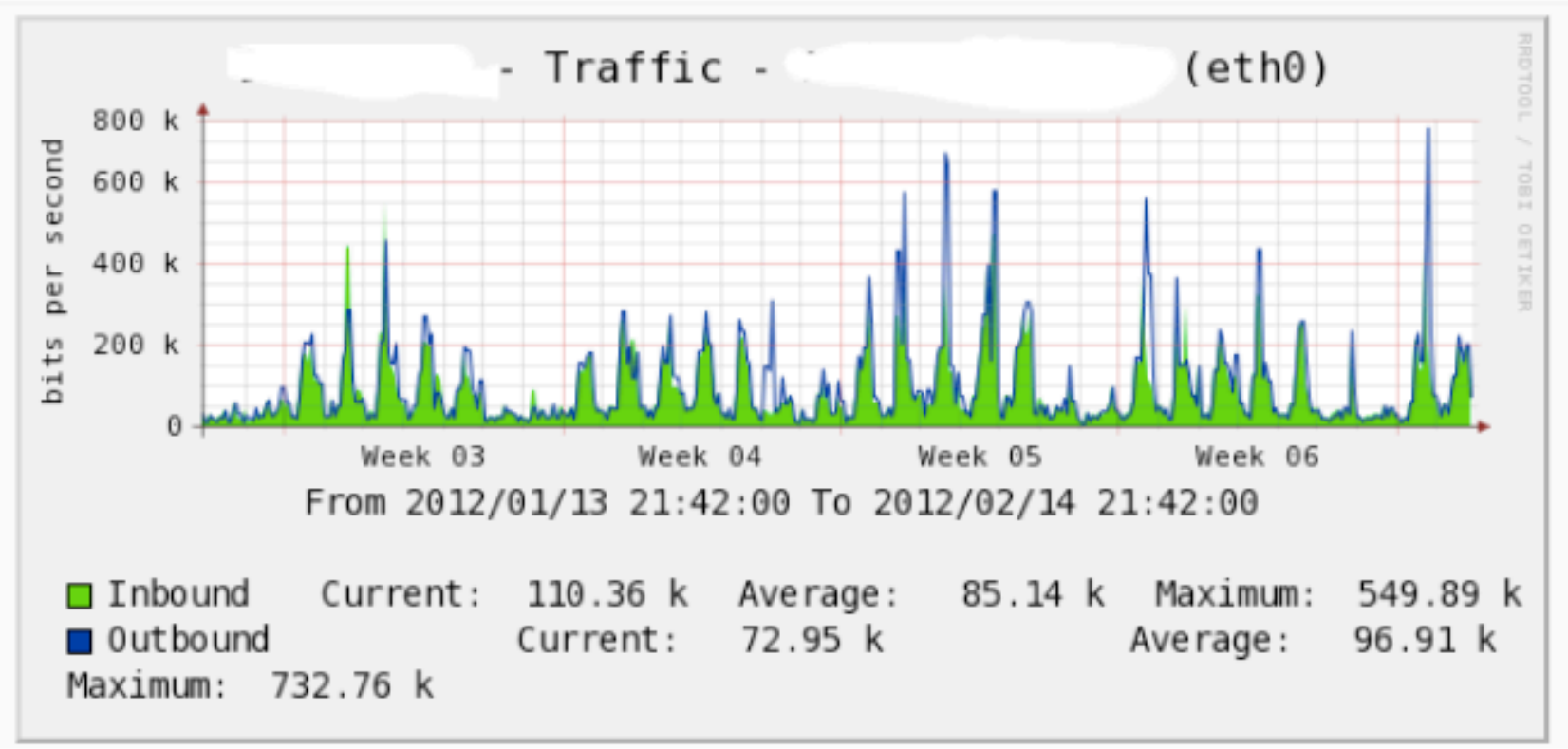


"Cacti is a complete frontend to RRDTool, it stores all of the necessary information to create graphs and populate them with data in a MySQL database. The frontend is completely PHP driven. Along with being able to maintain Graphs, Data Sources, and Round Robin Archives in a database, cacti handles the data gathering. There is also SNMP support for those used to creating traffic graphs with MRTG."

Initial Graphs



Over time you'll see tendencies



Demonstration of Tools

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

Log Management

- Centralize and consolidate log files
- Send all log messages from your routers, switches and servers to a single node – a *log server*.
- All network hardware and UNIX/Linux servers can be monitored using some version of `syslog`.
- Windows can, also, use syslog with extra tools.
- Save a copy of the logs locally, but, also, save them to a central log server for security and ease of inspection
- Watch your log files:
  - It's not practical to do this manually

Syslog basics

Uses UDP protocol, port 514

Syslog messages have two attributes (in addition to the message itself):

Facility			Level	
Auth	Security		Emergency	(0)
Authpriv	User		Alert	(1)
Console	Syslog		Critical	(2)
Cron	UUCP		Error	(3)
Daemon	Mail		Warning	(4)
Ftp	Ntp		Notice	(5)
Kern	News		Info	(6)
Lpr			Debug	(7)
Local0 ...Local7				

Log Management and Monitoring

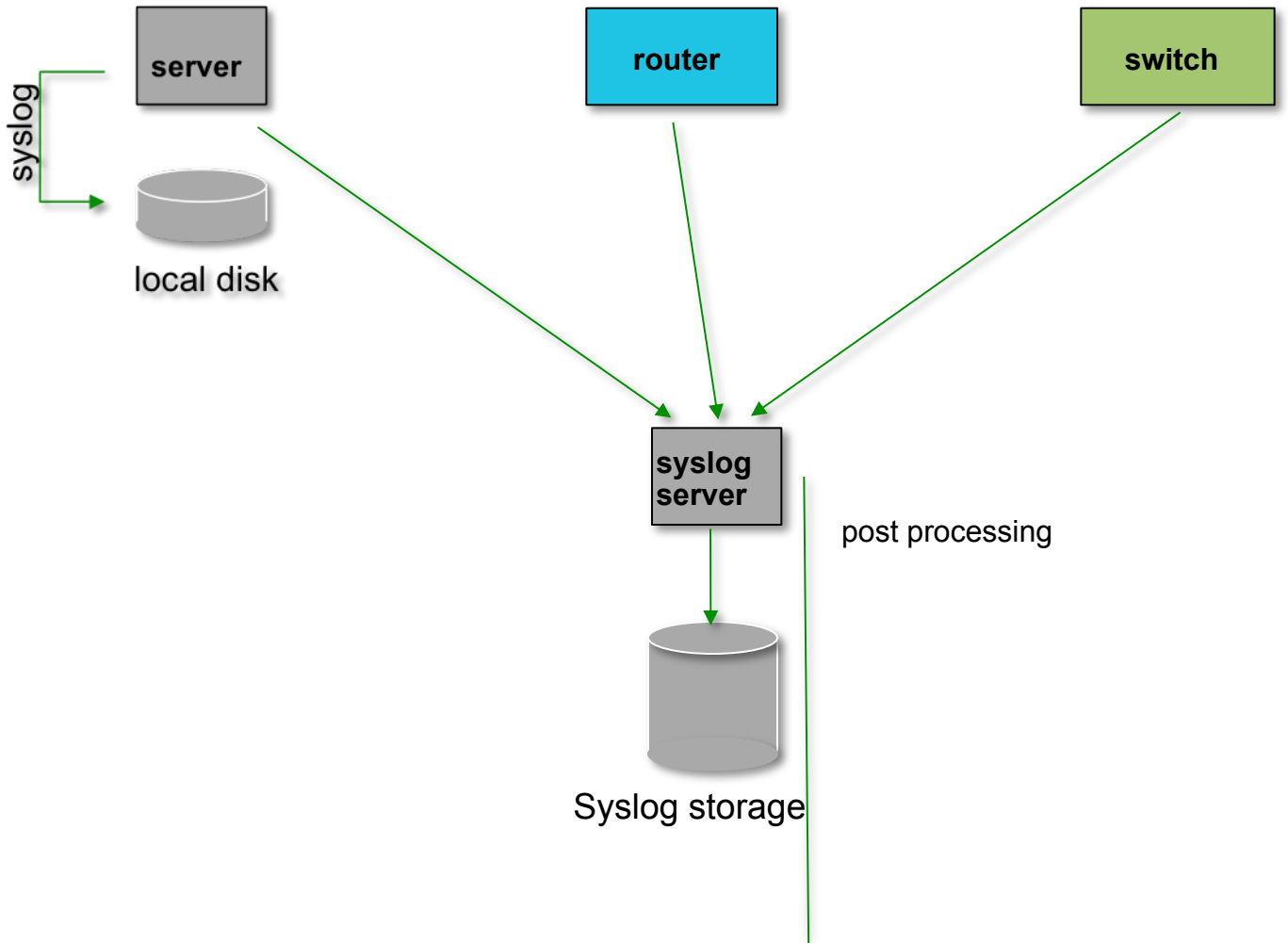
On your routers and switches

```
ep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

ep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console
by pr on vty0 (203.200.80.75)

CI-3-TEMP: Overtemperature warning

ar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed
state to down
```

And, on your servers

```
ug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

ug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from
169.223.1.130 port 2039 ssh2
```

Centralized logging



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/

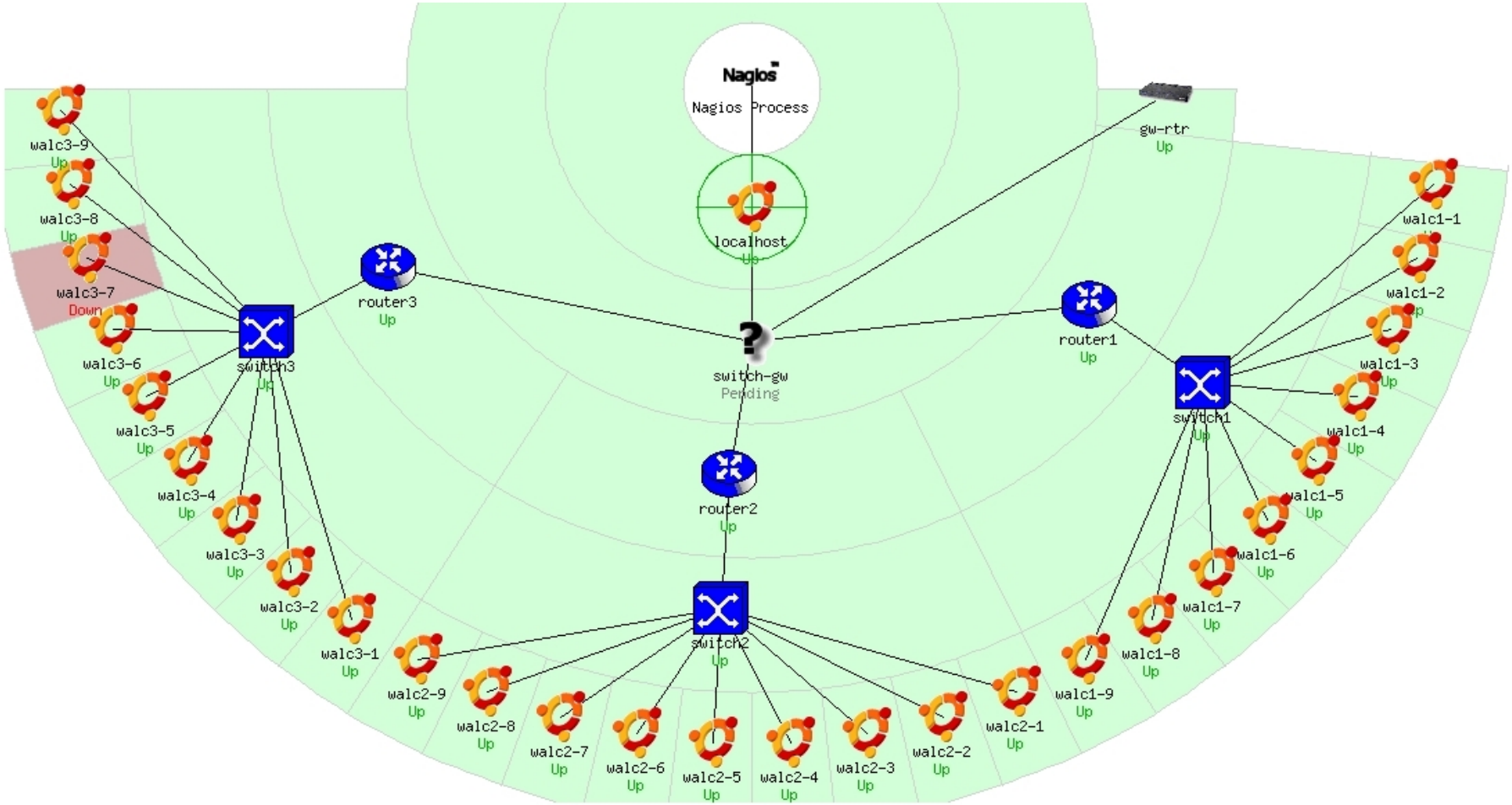
Features

- 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

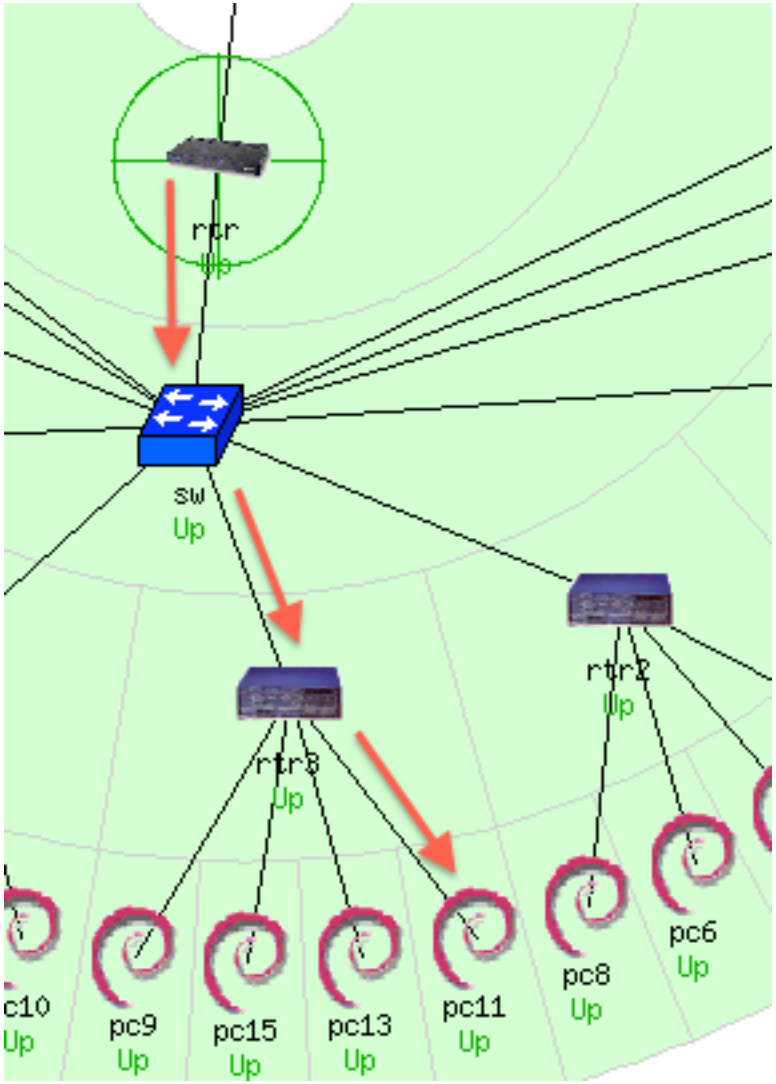
Features cont.

- 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

What is RANCID

The ”Really Awesome New Cisco config Differ” – Really!

A configuration management tool:

- Keeps track of changes in the configs of your network equipment (Cisco, HP, Juniper, Foundry, etc.)
- Works on routers and switches

What is RANCID?

Automates retrieval of the configurations and archives them

Functions as:

- Backup tool - ”woops, my router burned”
- Audit tool - ”how did this error get in?”
- Blame allocation :) - ”who did it?”

The data is stored in a VCS (Version Control System) – supported are:

- CVS (Concurrent Versions Systems)
- SVN (SubVersioN)

How does it work?

Run (manually or automated)

Lookup list of groups

For each device in each list of groups

- Connect to the equipment (telnet, ssh, …)
- Run ”show” commands – config, inventory, ...
- Collect, filter/format data
- Retrieve the resulting config files
- CVS check-in the changes
- Generate a *diff* from the previous version
- E-mail the diff to a mail address (individual or group)

What to use it for

- 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 (anyone have stories?)

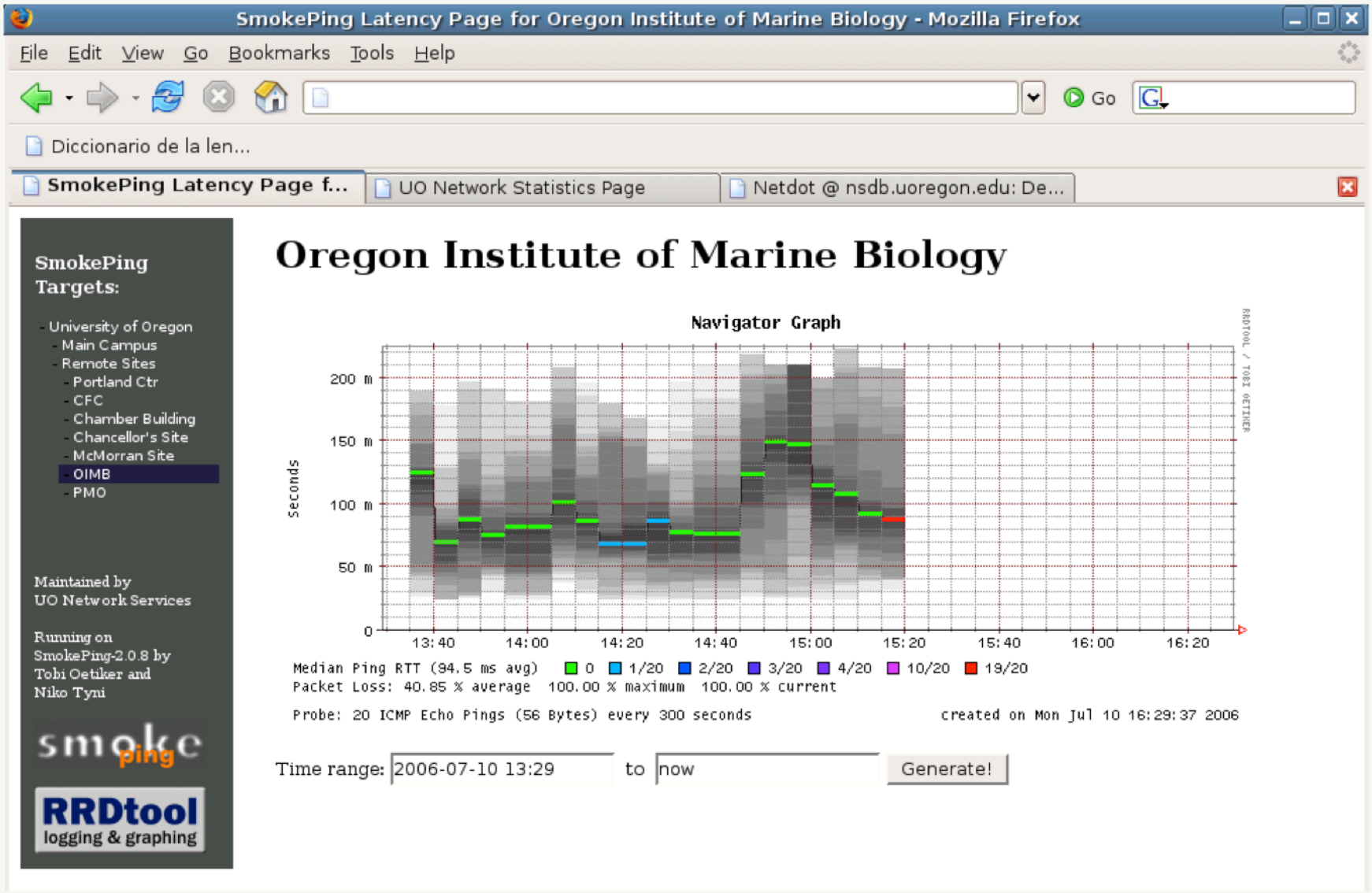
Demonstration of Tools

- 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”



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.

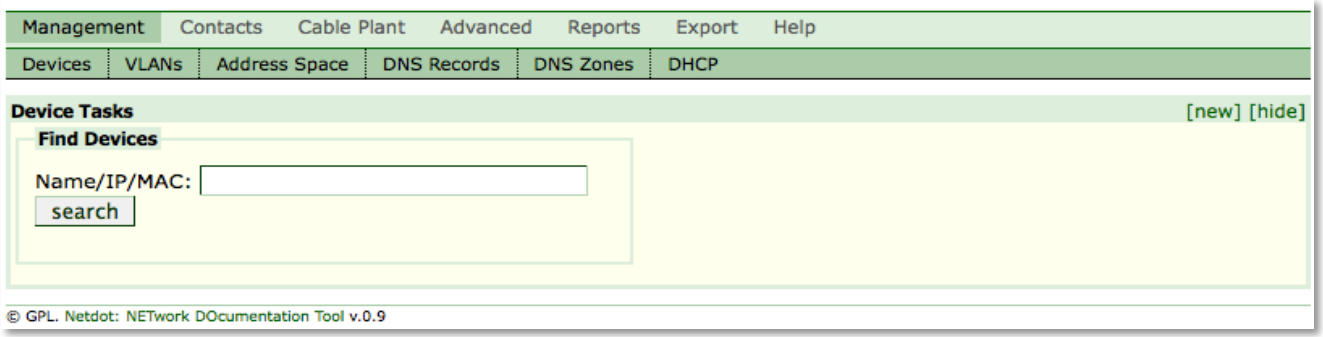
Core functionality includes:

- 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.



Questions?

?

A few other tools

iperf, bandwidthd, perSONAR, mtr, nmap, wireshark, tcpdump, …

Network Intrusion Detection (NIDs):

- **SNORT** - a commonly used open source tool: http://www.snort.org/
- **Prelude –** Security Information Management System https://dev.prelude-technologies.com/
- **Samhain –** Centralized HIDS http://la-samhna.de/samhain/
- **Nessus** - scan for vulnerabilities: http://www.nessus.org/download/
- **OpenVAS**