DSC - Development

by
Carl Olsen & Johan Ihrén
calle@autonomica.se

Autonomica and me

- Operate `i.root-servers.net` (anycast from 30+ locations) and a number of TLDs (unicast and/or anycast)
  - Total number of nameservers “more than a handful”
- Management and ops in Stockholm, Sweden
- I’m working as systems developer at Autonomica with DSC as a primary interest

Short Introduction to DSC

- DSC - DNS Statistics Collector
- Originally created by Duane Wessels
- In use across the Internet by growing numbers of organizations
- Another branch developed at Autonomica (by me) as a result of our operational requirements

Recap of DSC

- Original DSC consists of
  - Collector - collects DNS Data
    - Process near the DNS server(s)
  - Presenter - presents the collected data
    - Process near the stats consumer

Original Collector

- Capture packets using pcap-lib
  - similar to what tcpdump does
- Collects statistics (i.e. data reduction)
  - saves stats in XML format on local disk
- Separate process sends data to the presenter over **`https`** or **`rsync`**/**`ssh`**
- Static configuration
  - Need restart to reread configuration

Autonomica Version

- Threaded instead of forked
- Able to remotely configure the collector
  - use a dedicated SSL tunnel for security
  - use an XML-based command language.....
  - e.g "`reconfigure`","`status`","..."

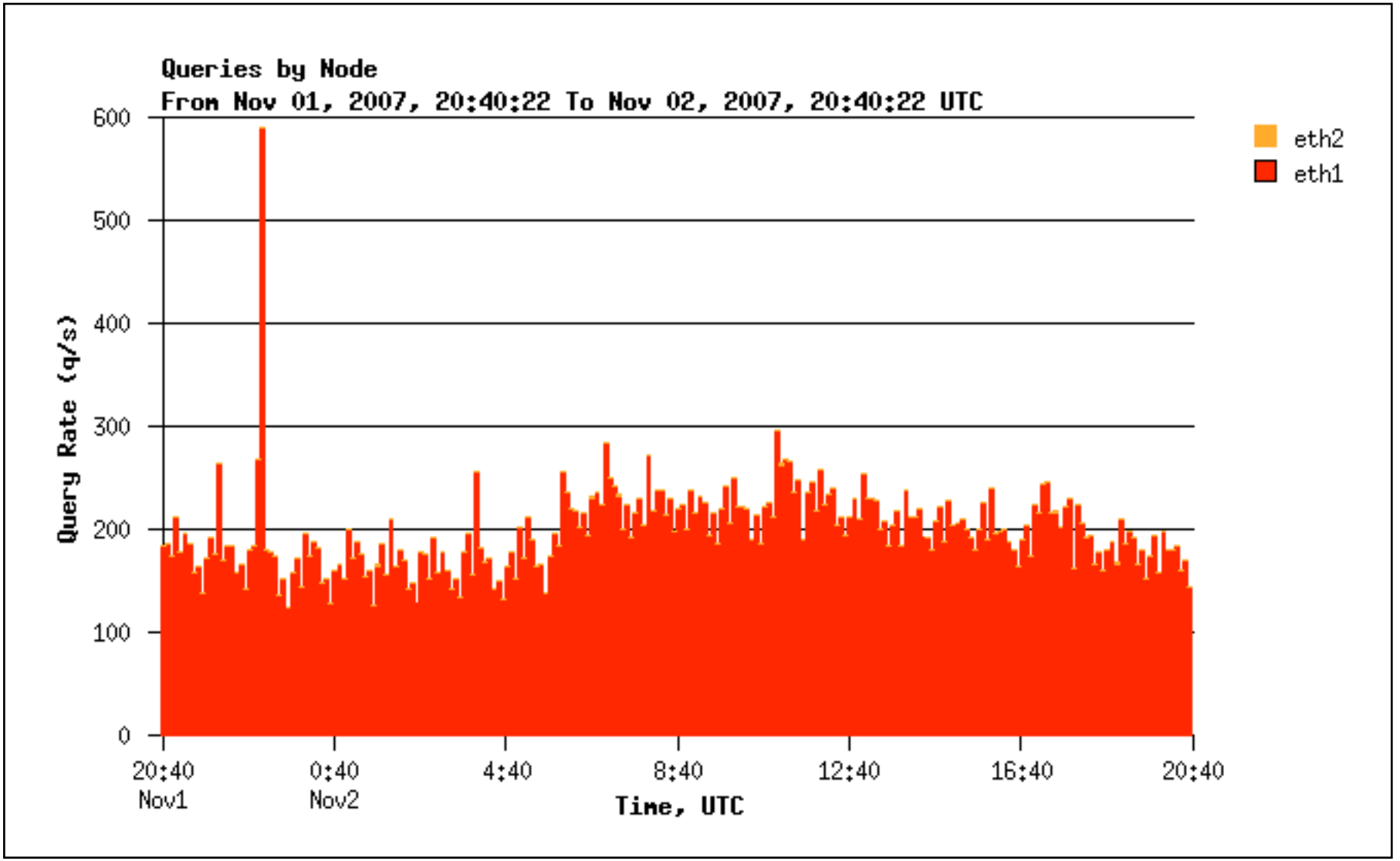
dns2db

- Developed by Autonomica (under contract for .SE)
  - Reads pcap-files and stores DNS information in a **`sqlite`** database
  - sql statements for analyzing DNS data
    - enables deep packet analysis
    - there exists some kind of GUI...
- Uses either pcap or libtrace (compile time option

Systems Analysis

- Both system works in their own domain
  - DSC - good for an overview
  - **`dns2db`** - to focus on specific details
- They complement each other in a great way
- Unfortunately these are two different systems

Example from AS112



Close up analysis

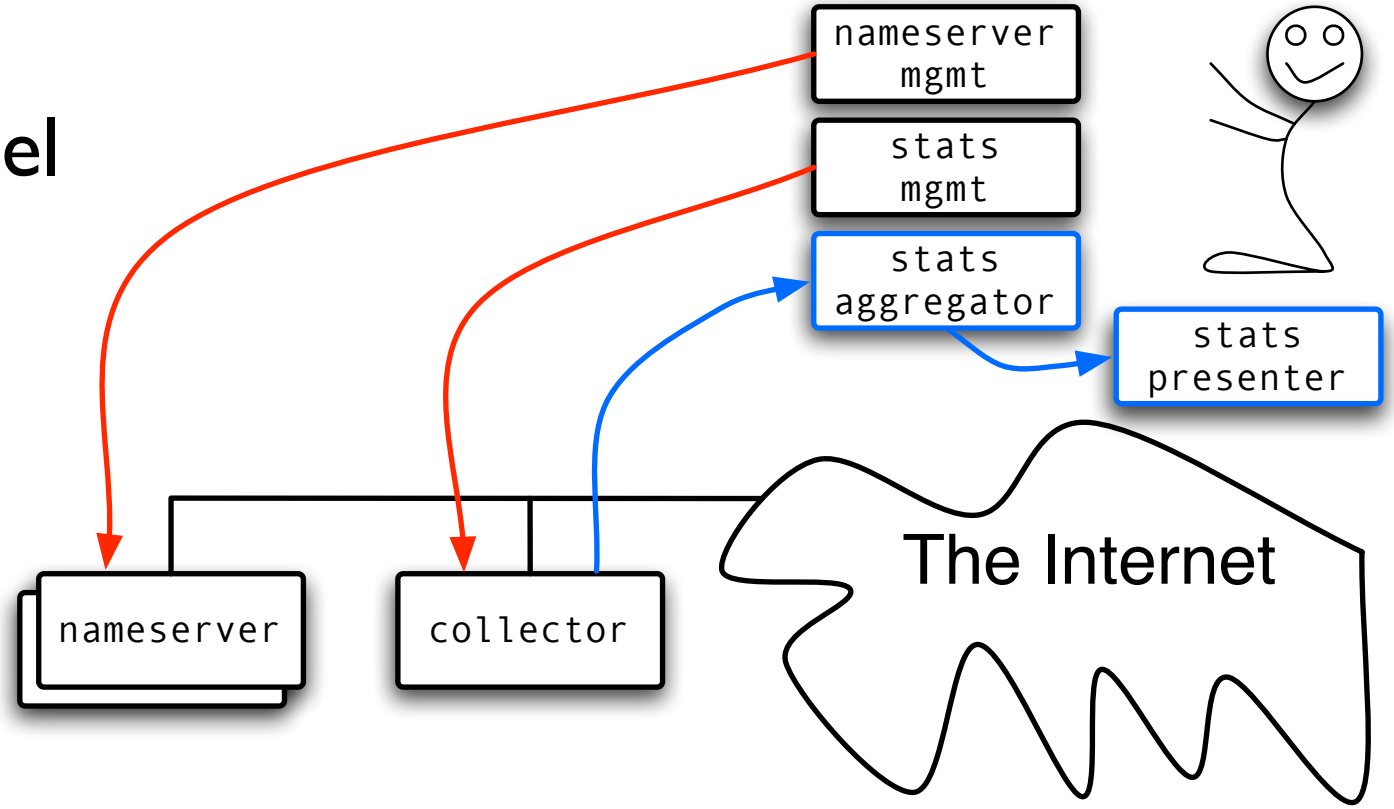
Date	Time	q/m
20/10	23:50	11792
20/10	23:55	18220
21/10	00:00	50078*
21/10	00:05	17185
21/10	00:10	16098

Further Analysis

- dns2db gave me detailed facts
- Time (00:00)
  - select opcode from q group by opcode;
    - 0 - Query
    - 5 - Updates
  - select opcode,count(id) from q group by opcode;
    - 0|122936 about 60% of all queries
    - 5|92776 about 40% of all queries
- At another time (01:05)
  - select opcode from q group by opcode;
    - 0 - Query
    - 5 - Updates
  - select opcode,count(id) from q group by opcode;
    - 0|51987 about 75%
    - 5|17150 about 25%
- Why so many updates at 00:00??

Today (more or less)

- Proven model
- Has some limitations

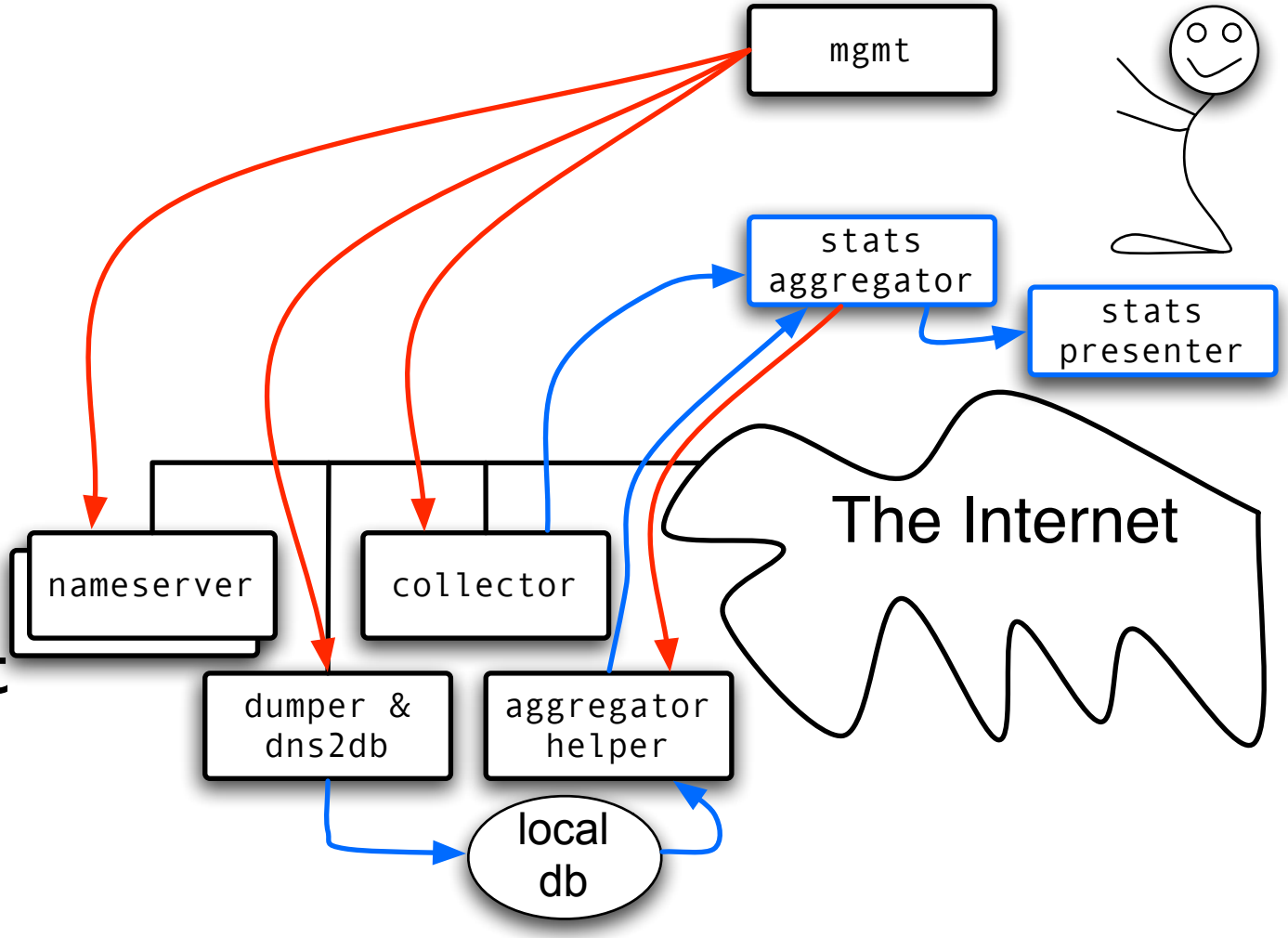


Future Needs

- One system with both functionalities consisting of
  - Collector (but it needs more fine-grained real-time control)
  - Aggregator (but it needs to sprout ability to extract data remaining at local sites)
  - Presenter (hmm, also needs improvement)
  - Management (exploding complexity)

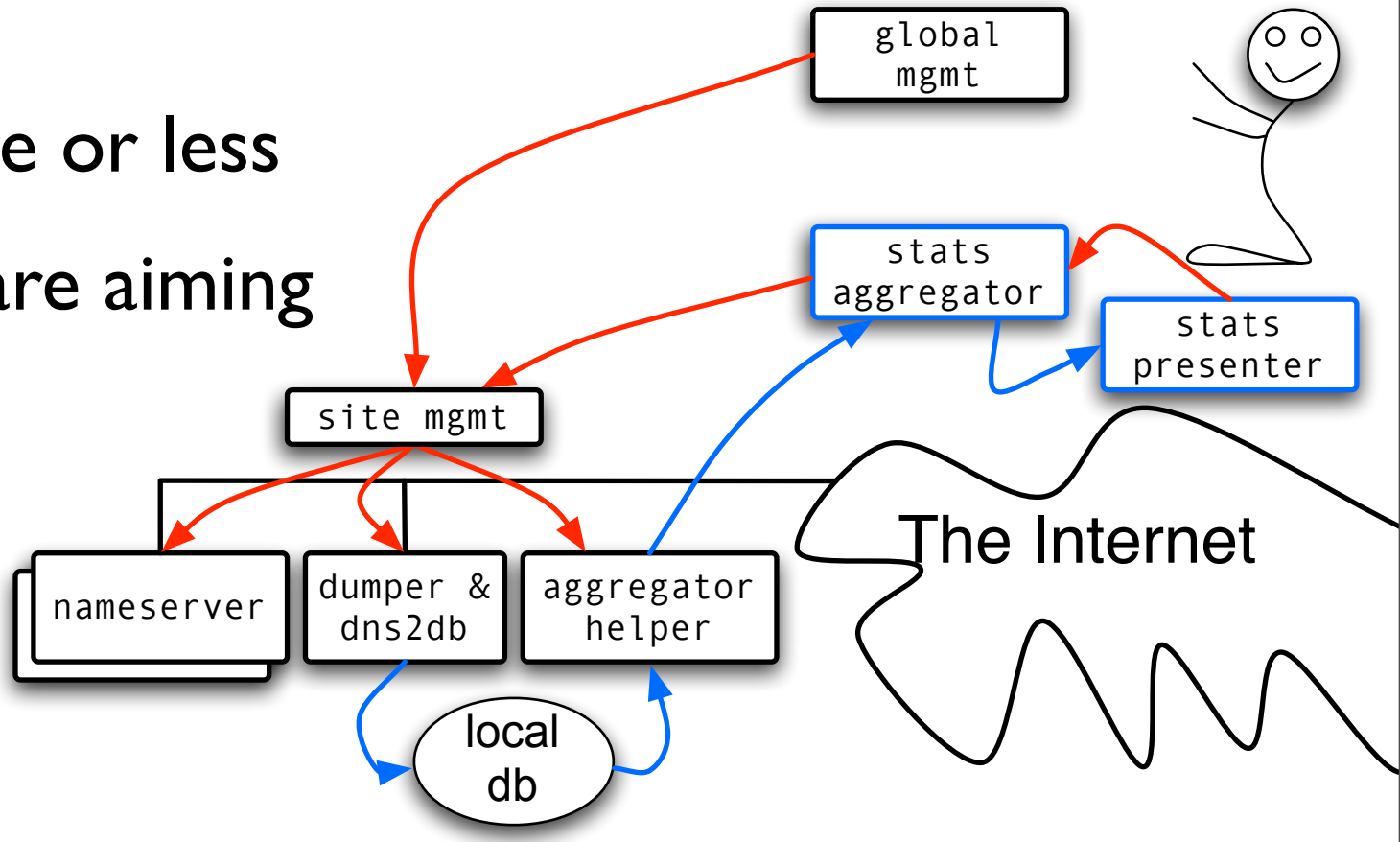
Next iteration

- Not really optimal
- Mgmt complexity growing fast



More re-writing

- This is more or less where we are aiming right now



Stats aggregator

- The basic idea of the aggregator is:
  - The presenter retrieves data from the aggregator when needed
  - The aggregator retrieves its data from the "aggregator helper" on each site if not stored
- The aggregator has some sort of storage, like a long lasting cache

Presenter

- Still under construction...
- Should be possible to have two modes:
  - Dynamic graph's
  - Analysis mode of data

Aggregator Helper

- Basic idea of the aggregator helper:
  - Short term storage
    - Pool of round-robin sqlite db's
    - Or pcap files...
- Retrieves the information from the db's
- This is the communication API to the aggregator or who ever wants the information
  - The idea is to use standard sql queries.

dumper & dns2db

- It should be possible store data in either sqlite format or as pcap format
  - The switch can be made on the fly
- Not only be able to store DNS traffic, but all traffic

Site managment

- Basic idea of site management box:
  - Engine to keep track of all the other “boxes”
  - Communication channel from the “Outside” world
  - Be able to do configuration and management of the other “boxes”

Finally!!!

- Most of this stuff is under construction
- Will be subject to changes
- But the overview aim is towards this

TQO

- Thanks!
- Questions?
- Or I'll sit down...

calle@autonomica.se