Nameserver Alternatives:
about NSD and Unbound

Wouter Wijngaards
wouter@nlnetlabs.nl (NLnet Labs)

Overview

- Introduction
- NSD
  - Features
  - Architecture
  - Performance
- Unbound
  - Goals
  - Architecture
  - Performance
- Summary

Introduction

- Monoculture is vulnerable
  - Alternative DNS servers to have code diversity
- Good alternative needs to be
  - Highly portable
    - OS and hardware diversity
  - Full RFC compliance
  - DNSSEC aware, IP6 ready
  - Open source (BSD license)
- About NLnet Labs
  - Foundation, not-for-profit

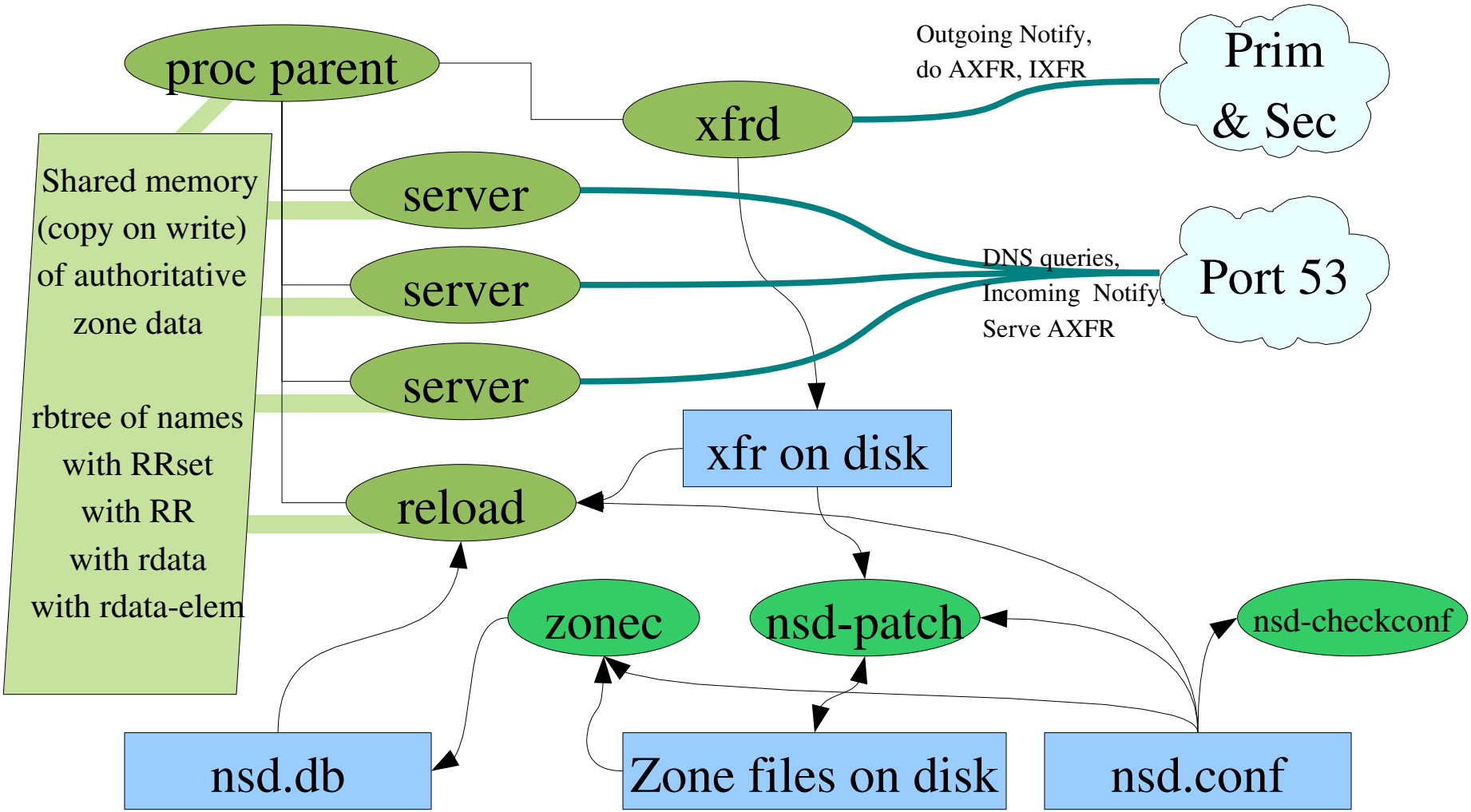
NSD

- Authoritative Server
  - Lean and mean
    - Only authoritative. Limited Statistics. User is smart.
  - Less code means less security problems
  - Less code means faster
- Feature buzz
  - Chroot, DNSSEC, NSEC, NSEC3, TSIG, IPv6
  - High performance, like 200k queries/second
  - Primary and secondary(AXFR, IXFR, NOTIFY)

NSD ctd.

- Status: 3.0.6 stable.
- Architecture:
  - Server processes use a precompiled copy-on-write database in memory to answer queries
  - Zone parsing, loading and transfer performed by separate processes from actual DNS server
- Deployed on root, TLD servers, like .se
- Get it
  - http://nlnetlabs.nl/nsd, or use package installer

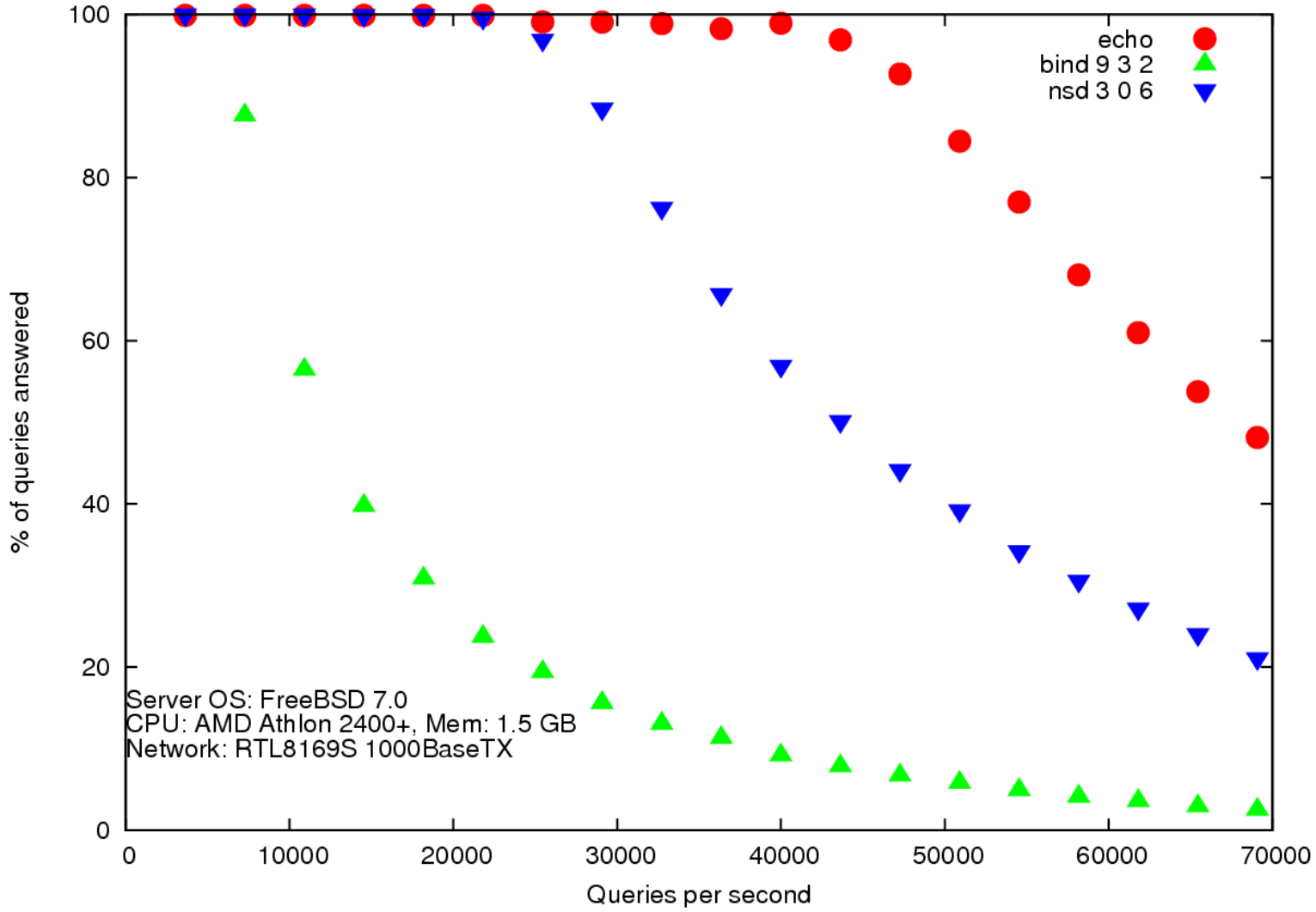
NSD 3 Architecture



NSD Tested

- Operating Systems
  - Solaris 9, 10
  - Linux
  - FreeBSD 6.2
  - Mac OS/X 10.4
- Hardware
  - i386, 32/64
  - Powerpc, Alpha
  - Sparc64
- Interoperability
  - Wire differences
    - with Bind 8, 9
  - Interop. OK
  - Details documented

NSD performance



NLnet Labs

Unbound

New!

- Goals
  - open source DNSSEC validator
    - alternative validator choice for BIND 9
  - Validating caching recursive server
  - Validating stub resolver library
  - POSIX C (portable Linux, Solaris, *BSD, ...)
  - BSD license
    - Promote deployment
  - High performance (even with validation)

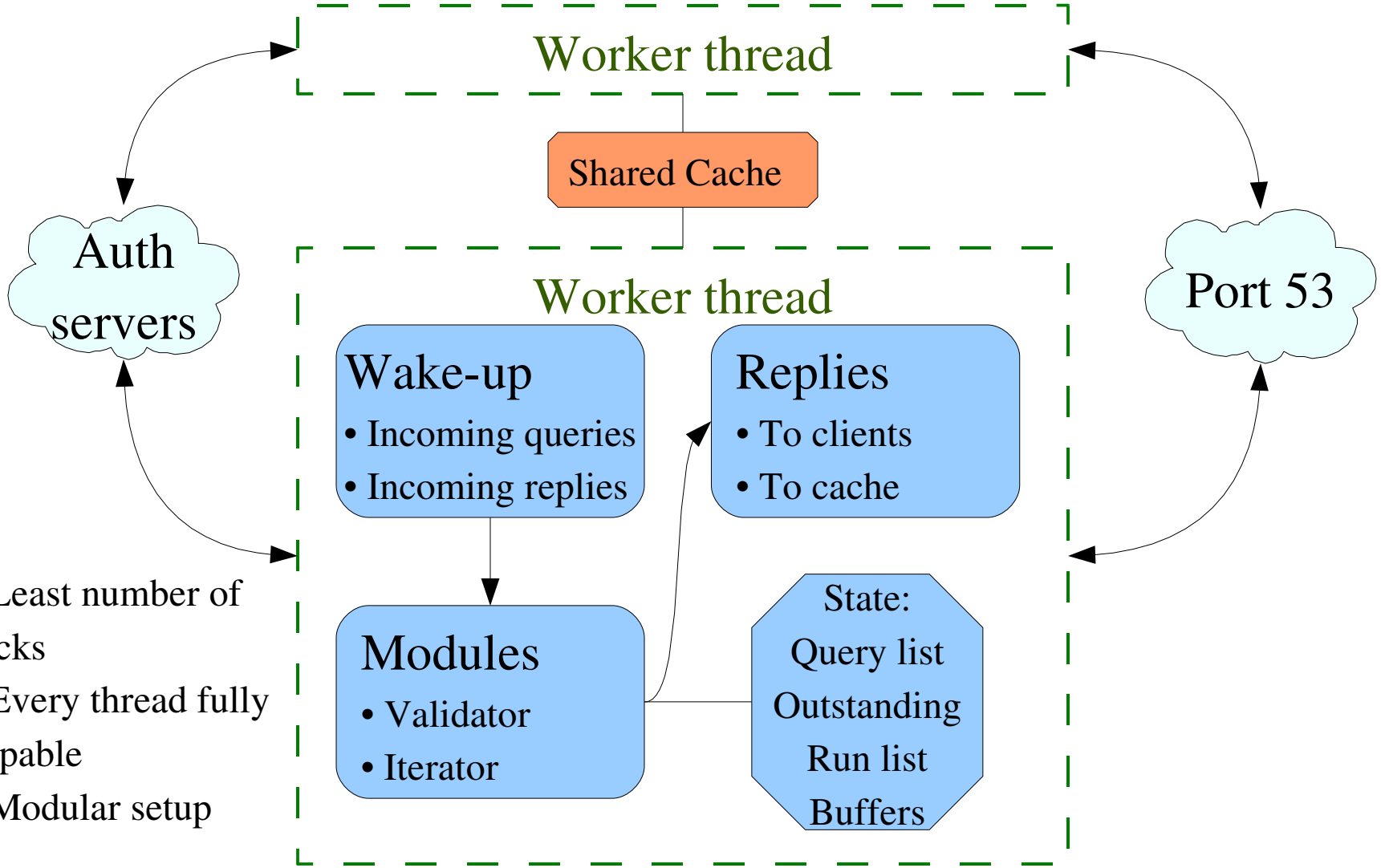
Unbound ctd.

- Feature buzz
  - Chroot, DNSSEC, NSEC, NSEC3, Ipv6, TSIG
  - Multi-threaded
  - Cache memory usage can be controlled
  - Cache poisoning/spoof resistance
    - Out of zone data is removed from messages
    - ID and port randomization, can use many (10k) ports
  - What do you need for operations?
    - wouter@nlnetlabs.nl mail me your ideas

Unbound ctd.2

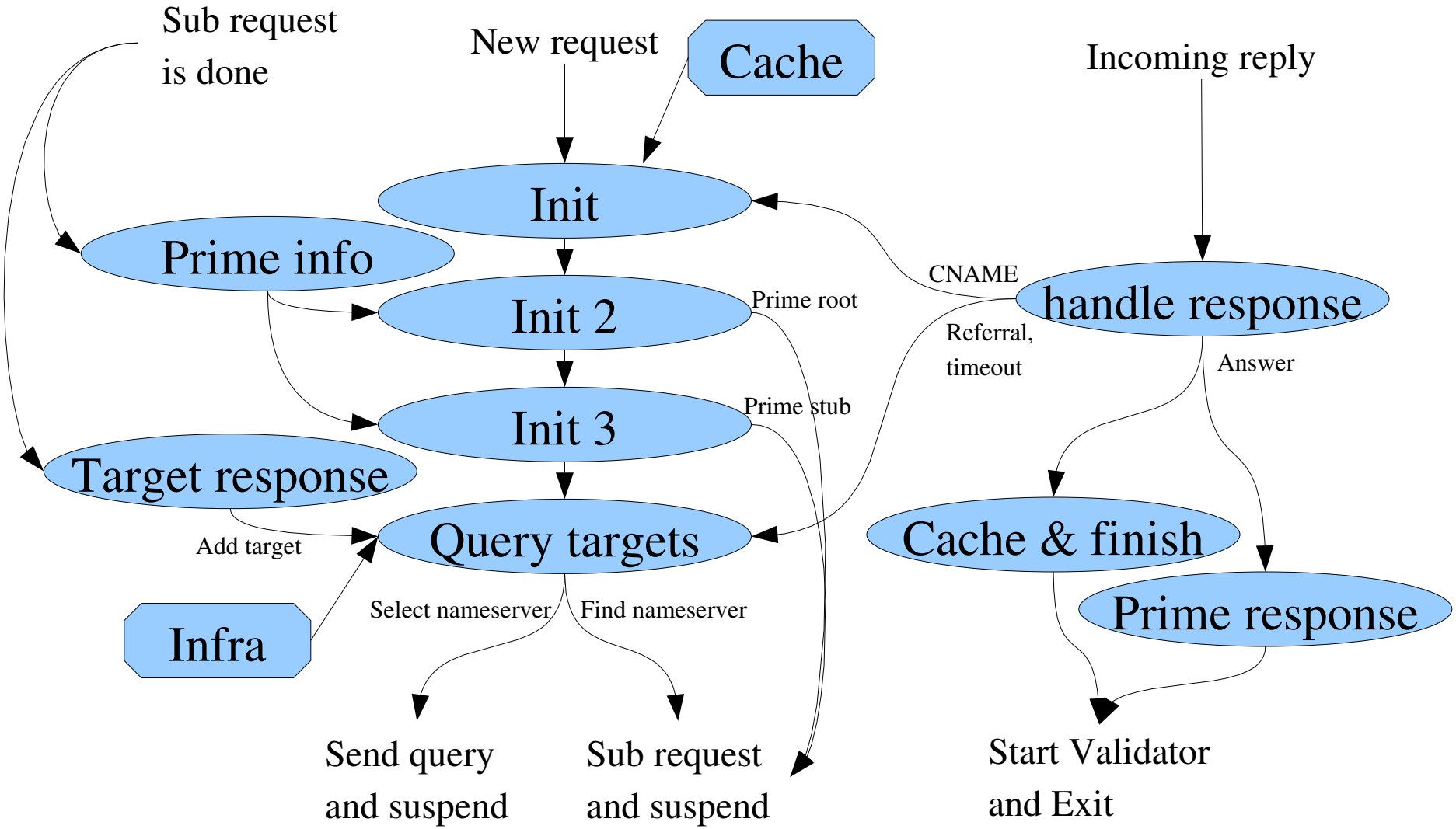
- Status: Prototype works
  - Code improvement; Test deployment
- Architecture
  - Worker threads access shared hashtable cache
  - Modular design, state machines work on query
- Deployment targets
  - Workgroup local DNS resolver
  - Large caching resolver installation (ISP)
  - Validating library for applications

Unbound Architecture

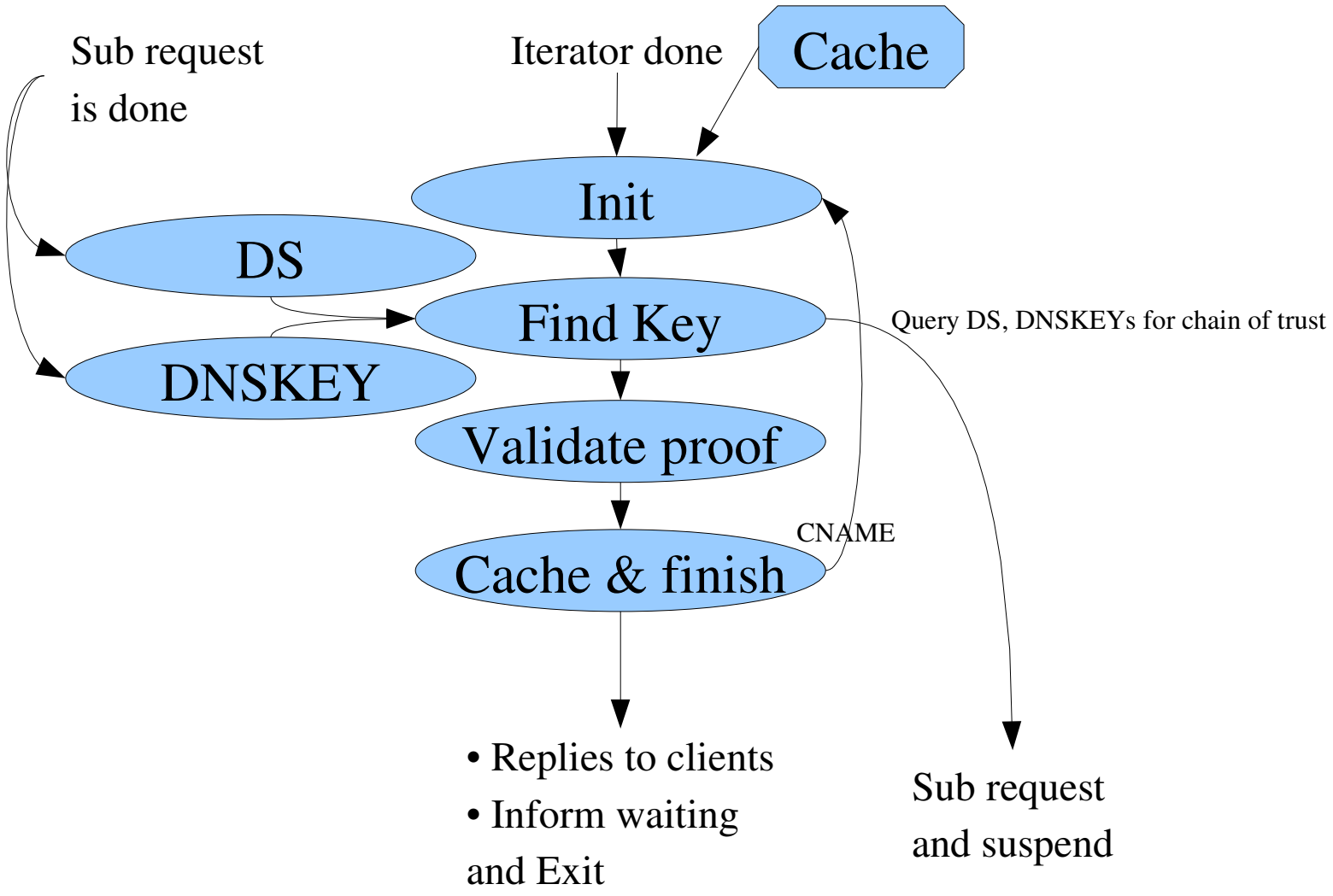


- Least number of locks
- Every thread fully capable
- Modular setup

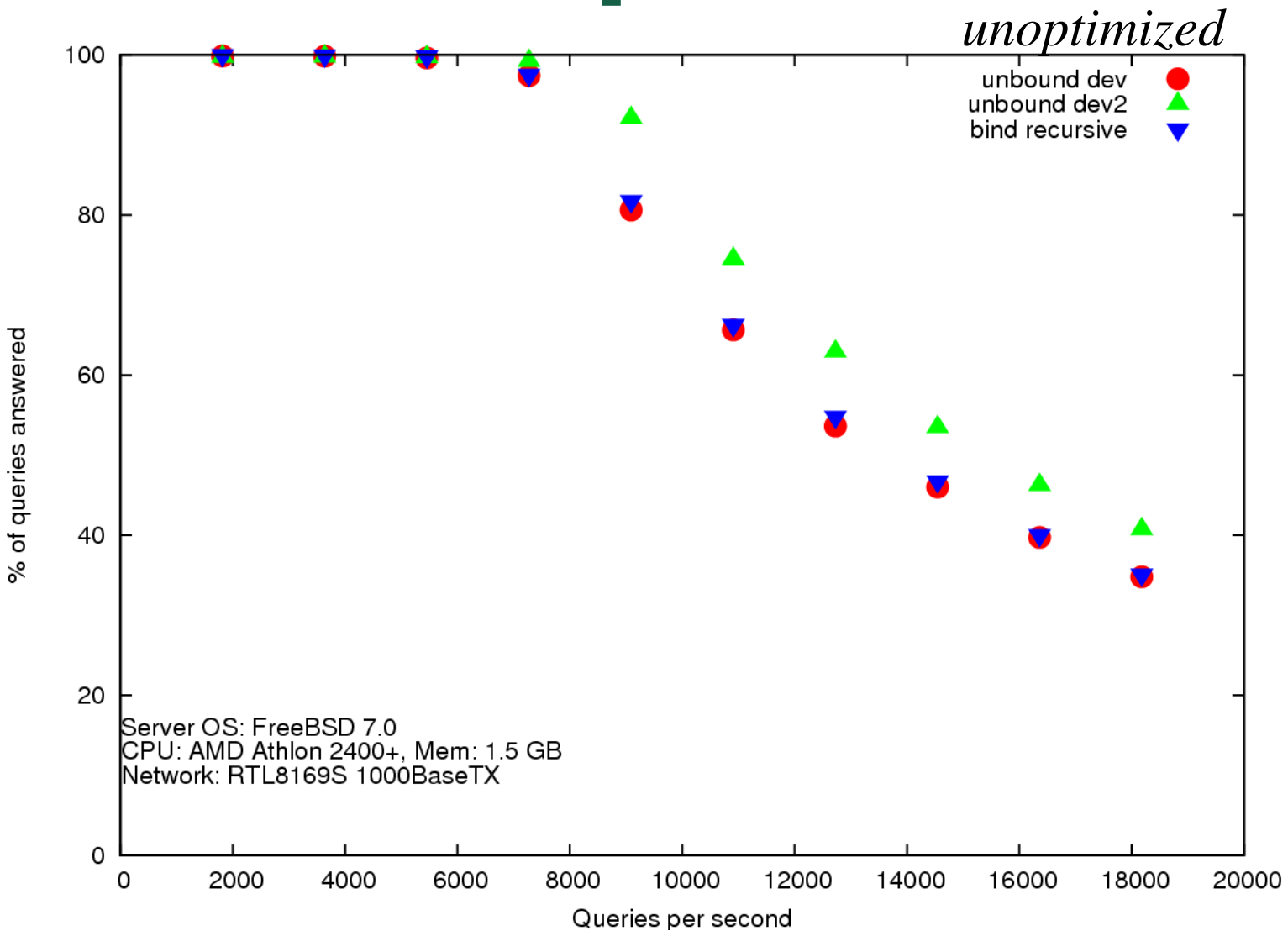
Iterator Module



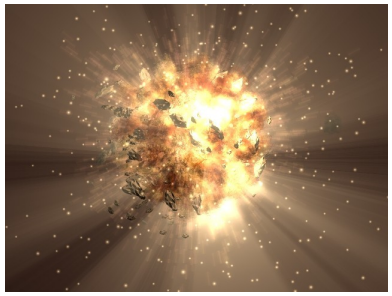
Validator Module



Unbound performance



Unbound Beta Test



- Volunteers wanted
  - For early beta testing
    - We do not know its performance in a real life, busy environment
      - Run shadow for real resolver initially
      - First tests, sure to run into problems
    - Memory, Speed performance.
    - Bugs and operational features.
- Mail me to sign up
  - wouter@nlnetlabs.nl

Summary

- DNS server choices
  - NSD – Authoritative DNS server
  - Unbound – Recursive DNS server
- Features
  - Open source
  - DNSSEC
  - standards compliant
  - high performance