NLnet Labs

Annual Report 2014

For an Open Internet

1 Highlights

NLnet Labs promotes and contributes to a stable and reliable Internet infrastructure, where DNS and inter-domain routing are key components of the infrastructure. The authoritative name server NSD 4 was initially released late 2013, and with NSD 4.1, released in 2014, a mature and stable upgrade for the proven NSD 3 is available. Unbound 1.5 and newer releases have been made available with useful features for improved integration with other systems like NetworkManager or NAT64 (to allow IPv6-only clients to access IPv4-only services).

The OpenDNSSEC project was transferred from OpenDNSSEC AB (svb) to NLnet Labs. With the transfer, NLnet Labs takes full responsibility for continuing the activities of both the OpenDNSSEC software and project as well as the support activities previously managed by OpenDNSSEC AB. Open Netlabs BV will take responsibility on the commercial aspects of the OpenDNSSEC project.

In collaboration with Verisign, we worked on the implementation and promotion of the getdns API library. This library allows application developers to use DNS security (DNSSEC) and other powerful new DNS features, and to include innovative security solutions in their applications.

The routing (configuration) toolset project ENGRIT started off with work on routing policy language RDL (routing documentation language). The kick-off of the SAND (self-managing anycast infrastructures for DNS) project was in December 2014. Together with SIDN Labs and Universiteit Twente, we explore scalable and robust methods for managing and monitoring dynamic anycast networks, with the aim to increase stability and security of the service.

In the area of technical governance, we contributed to the cross community working group (CWG) in the ICANN, that develops plans—as one of the multistake-holder organizations—for the IANA function transfer.

Education and research are important activities for NLnet Labs' signature. We contributed to colloquia and practicums (lab sessions), and hosted six interns during 2014.

All our efforts and deliverables are directed to strengthen the open and innovative nature of the Internet for all, and add to the security and stability of the core of the Internet infrastructure.

2 Areas: DNS and DNSSEC

The topics DNS and DNSSEC are strongly embedded in NLnet Labs' activities. Besides the well-known and widely adopted DNS name servers and DNS libraries developed by NLnet Labs, the OpenDNSSEC project was transferred in 2014 to NLnet Labs. Our activities focus on the development and maintenance of tools that facilitate the provisioning and use of DNSSEC, and as such we lower deployment barriers of a technology that will allow for further innovation of global Internet security mechanisms.

By developing alternative implementations of name-servers we also increase the stability of the DNS by offering diversity in code-base.

DNSSEC is one of the few enabling technologies that allows for the introduction of end-to-end authentication and confidentiality solutions. We see it as being a critical component to contributing to the increase in trust in the use of the Internet. Development, deployment, and innovating on top of DNSSEC deployments take a long, multi-year, potentially multi-decade, breath.

Besides development of software, we continue to invest effort in research projects to answer operational, technical, and theoretical questions about DNS security, architecture, operations, and deployment.

2.1 Provisioning of DNS Server-Side

2.1.1 NSD

NSD is NLnet Labs' authoritative name server and designed to be light-weight, high-performance, secure, and single purpose. NSD 4 is one of our flagships and was released in October 2013. With this new major release, NSD 4 has a number of modern features that makes it usable for a broader set of users.

Goals

NSD 4: provide a stable and high-performance authoritative DNS server for a larger, more diverse set of users. Besides improved performance, reduction of memory usage (memory footprint).

NSD 3: continue to support NSD3 as a secure high-performance name server.

NSD 4 Activities

NSD 4 has become the primary development release of the NSD name server. From experience and feedback in 2014, NDS 4 has shown to be a stable and reliable replacement for NSD 3. With NSD 4.1 some major features and memory usage improvements have been realized, making it a practicable upgrade for operational environments that now rely on NSD 3.

NSD 3 Activities

NSD 3 is now in maintenance mode, with mainly bug fixes and incorporation of some new RR types and a small performance improvement in parsing/writing zone files.

Results

The initial NSD 4.0 release has seen a number of bug fix releases NSD 4.0.1 to NSD 4.0.3. The main new improvements were introduced in version NSD 4.1, released in September 2014. Memory usage has been reduced with 50% in the "no database" mode. The new feature to reduce memory footprint is described in a blog post. Other features were added to integrate NSD 4 more easily in operational environments. Also new RR types are implemented as defined in RFC 6844 and RFC 7043.

NSD 3.2.17 and NSD 3.2.18 implemented similar to NSD 4 the new RR types defined in RFC 6844 and RFC 7043. This in addition to regular maintenance features.

Impact

NSD clearly serves its design goals: to provide an alternative implementation to authoritative DNS servers in order to increase resiliency and stability of the global DNS infrastructure: NSD is used on root servers such as the L and K root servers and many top-level domain registries, including .NL, .DE, .BR, .SE, and .UK. The main motivations for running NSD are high-performance, stability, and to have code diversity within the installed base.

Besides providing a reliable and high-performance name server, NSD 4 is also a reference implementation of relevant IETF RFC standards. By realizing reference implementations, we also contribute to the standardization process by communicating our experiences and sending feedback to the community.

2.1.2 DNSSEC Zone and Key management: OpenDNSSEC

OpenDNSSEC is a turnkey solution for DNSSEC management that hides the complexity of DNSSEC and enables an effortless deployment in operational environments. The DNSSEC zone management system takes unsigned zones, adds signatures and other records for DNSSEC and passes it on to the authoritative name server. Furthermore, the DNSSEC key-maintenance expert system supports all documented key rollover scenarios and allows flexibility in operation varying from one key maintenance policy for all zones to per-zone configuration and maintenance.

In June 2014, the OpenDNSSEC project was transferred from OpenDNSSEC AB (svb) to NLnet Labs. With this transfer, continuity of the project is now guaranteed by NLnet Labs.

Goals

Continue the maintenance of OpenDNSSEC version 1 branch and address release management of version 2. To get OpenDNSSEC 2 on track, the requirements document for version 2 needs reconsideration and milestones for deliverables need to be defined.

Activities

With the transfer of the OpenDNSSEC project to NLnet Labs, all development is done by NLnet Labs software developers. Project management for the remainder of 2014 was with Jakob Schlyter, Kirei. Jakob Schlyter was involved with the OpenDNSSEC project from the beginning and his guidance was important for an efficient and trouble free transfer of the activities to NLnet Labs.

OpenDNSSEC 1.4 has seen four releases in 2014. The releases 1.4.4 to 1.4.7 contain mostly bug fixes and some new features and improved functionality. An important new feature in OpenDNSSEC 1.4 is support for RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors. This is relevant for organizations that run their own root trust anchor, for example ICANN that plans root zone KSK rollover, but also organizations that run their own name space to meet security requirements. There was no official 1.4 release with RFC 5011 support in 2014, but the source is publicly available in the OpenDNSSEC repository.

OpenDNSSEC 1.3 is the Long Term Support (LTS) version of OpenDNSSEC. In 2014 two releases were made available that contained bug fixes and a number of improvements for operational robustness, but no functional extensions.

Development on OpenDNSSEC 2.0 was mainly in the first half year; after the transfer to NLnet Labs, focus was on the stable 1.4 release for continuity and support to community. In first half of 2014, the enforcer module has been refactored to meet the performance requirements for managing large number of zones. In the second half of 2014, most efforts were directed to control the project and define release milestones.

At the end of 2014, we appointed two new colleagues to the OpenDNSSEC project, amounting to three developers assigned to OpenDNSSEC in 2015.

Results

Publication of maintenance versions 1.4.4 to 1.4.7, and OpenDNSSEC 1.3.17 and 1.3.18 LTS. In addition to regular version updates, we have now RFC 5011 functionality available in the OpenDNSSEC 1.4 source repository branch. OpenDNSSEC 2.0 has seen two alpha releases for evaluation.

Impact

OpenDNSSEC has lowered the barrier to deploy DNSSEC: its availability has been contributing to positive decisions with respect to the deployment of DNSSEC. OpenDNSSEC has a number of high-profile users as listed at http://www.opendnssec.org/about/known-users/.

2.2 Client-Side Availability of DNSSEC

2.2.1 Unbound

Unbound is one of the main implementations for DNSSEC-enabled DNS resolution and thereby an important contributor to usability of DNSSEC.

Goals

Create a versatile, high-performance DNS resolver that can be incorporated at various places in software stacks, embedded, as default resolver in OS distributions, and primary resolver for (large) ISPs. Maintain stability, implement new IETF Internet standards, and include relevant operational requirements.

Activities

We continue the development of Unbound to have the recursive resolver fit in various setups and operational environments. We continue to be lenient towards feature requests, in part to foster the adoption of DNSSEC (-validators).

The release of Unbound 1.5 in 2014 includes various improvements for integration with other systems like NetworkManager and dnssec-trigger, but also for running Unbound on Windows. Other noteworthy features are DNS64 support to be used in combination with NAT64 to allow for a IPv6-only client to initiate communications by name to an IPv4-only service; and incorporation of dnstap, a flexible, structured binary log format for DNS software.

The implementation of the ‘client-subnet’ functionality[1] is actively used by a number of organizations, and feedback and fixes are incorporated in the source tree. Unbound with-client-subnet functionality is available from a specific branch in the public source repository

Results

Publication of versions 1.4.22, and 1.5.0 and 1.5.1. Full functioning release of the client-subnet branch.

[1] -https://tools.ietf.org/html/draft-ietf-dnsop-edns-client-subnet-00

Impact

Unbound is acknowledged as a leading implementation of a secure and stable DNSSEC validator. The software is used in various high-profile and high-available environments, amongst them various large ISPs, as a standard resolver in some OS distributions, and in several DNS appliances.

Besides the FreeBSD project, the OpenBSD project now also uses Unbound as the default resolver starting with the version 5.6 release of the system.

2.2.2 DNSSEC Trigger

DNSSEC Trigger is an effort to cope with the 'DNSSEC last mile' problem. In order to be able to rely on DNSSEC validation one wants to bring DNSSEC close to the application, preferably on the OS so that the benefits of DNSSEC are available for all.

Goal

Handle a number of corner cases that the software needs to deal with such as proper operation when the users bring up VPNs. Improve interaction with guest operating systems like Mac OS X, BSD, Linux, and Windows, and integration with NetworkManager and systemd.

Activity and Results

We have been collaborating with various developers in the Fedora and Debian Linux community on a tighter integration with NetworkManager that is common between these distributions and for which we accepted multiple patches. This resulted in the release of DNSSEC trigger version 0.12.

Impact

Further understanding about the impediments to get DNSSEC to the end users: a bridging tool that sets an example for other initiatives to follow.

2.3 DNS Development Frameworks

The development of applications and services that execute their own DNS resolving and are DNSSEC-enabled is an important step forward in the security awareness of applications and services. With DANE and TLSA (RFC 6698), not only security improves but takes also privacy to the next level.

2.3.1 Secure getaddrinfo/getnameinfo (getdns API)

getdns is an asynchronous DNS API, which API specification is developed in collaboration with application developers. getdns API offers application developers a modernized and flexible way to access DNS security (DNSSEC) and alternative transport, like TCP pipelining, DNS over TLS, or STARTTLS for DNS (enhancing DNS privacy). A particular hope is to inspire application developers towards innovative security solutions in their applications.

Goal

Provide a modern asynchronous DNS API with the initial release of getdns API v0.1.0. Besides the development of the software, we generate some interest and traction of a new, alternative for getaddrinfo/getnameinfo that includes DNSSEC functionality for application developers and provide a modern (asynchronous) DNSSEC-enabled system stub resolver.

Activities

NLnet Labs worked in collaboration with Verisign Labs towards the design and implementation of the getdns API[2]. A first public release of getdns API v0.1.0 was made available in February 2014. With the first public release a number of subsequent releases were published with bug fixes, a number of improvements and new functionality. Occasionally the API needed some changes to comply with relevant RFCs. The API was originally edited by Paul Hoffman, but is now maintained by the getdns team[3].

Beside the development of the getdns API, a number of public presentations and events were organized to promote the adoption of the API.

Results

An initial public release of getdns API 0.1.0 in February, and updates up to release 0.1.5 in October 2014. Presentations at the IETF, RIPE, ICANN, OSCON 2014, and one of API providers in “The Hack Battle” at The Next Web 2014 conference. Hand-on tutorial at RIPE 69.

Impact

The presentations of getdns API at various events showed that there exists serious interest by the industry. In particular, where DNSSEC and DANE are relevant, getdns API is considered to be a serious option.

2.3.2 Ldns

Goal

Work towards a major version release of ldns version 2. Important goals are consistent support for getdns API and memory reduction (mainly for OpenDNSSEC).

Activity

The activities for ldns v2 are closely related with getdns API developments. The results of these developments that are related to the ldns library will be moved to the ldns v2 development repository.

The memory management of ldns is optimized and the time complexity of some operations in ldns are reduced. Additionally we resolved a number of bugs and added newly standardized features.

Results

Ldns v1.6.17 is published in January 2014. The development on ldns v2 is in the getdns API code base.

2.3.3 Net::DNS

Net::DNS is a DNS resolver implemented in Perl. It allows the programmer to perform nearly any type of DNS query from a Perl script. NLnet Labs will continue the maintenance and development of the Net::DNS suite.

Goal

Regular maintenance and continued clean-up of the architecture.

2-https://getdnsapi.net/
3-https://getdnsapi.net/spec.html

Activities

In collaboration with Dick Franks, one of the volunteer maintainers and main contributors to the code, a clean-up of the internals has been performed. In that process we occasionally had to change undocumented behavior, leading to breakage in 3rd party applications. Because of this we have proceeded with care but still had to issue emergency releases to counter unexpected breakage elsewhere.

Results

Releases 0.74 through 0.81 of Net::DNS and releases 0.18 through 0.21 of Net::DNS::SEC.

2.4 Other Activities

2.4.1 Measuring DNSSEC Validating Resolvers

Nicolas Canceill finalized his MSc. student research project “Measuring the Deployment of DNSSEC over the Internet”. In this study, Canceill measured the deployment of DNSSEC validating resolvers on the Internet using the RIPE Atlas measurement infrastructure. The results of the study are highly relevant to the community and complements other well-known studies by Geoff Huston and George Michaelson. The results and final report have been presented at the RIPE 68 meeting (Measuring the Deployment of DNSSEC over the Internet) and the DNSSEC Workshop at ICANN 50 (Measuring DNSSEC Validating Resolvers Using RIPE ATLAS).

2.4.2 Hackathons

- dnstap Hackathon, Amsterdam, The Netherlands, May 2014. Paul Vixie and Robert Edmunds visiting NLnet Labs.
- OpenBSD 2014 Hackathon, Ljubljana, Slovenia, July 2014. Discussing NSD and Unbound with OpenBSD coders and community.

2.4.3 IETF DNS activity

Results

DNS-Encryption BoF, presentation on Confidential DNS proposal, W. Wijngaards, IETF 89, London, England, March 2014.

Confidential DNS, draft-wijngaards-dnsop-confidentialdns, W. Wijngaards (NLnet Labs), G. Wiley (Verisign, Inc).

Publication of RFC 7129: Authenticated Denial of Existence in the DNS, R. Gieben and W. Mekking, February 2014. This document provides additional background commentary and some context for the NSEC and NSEC3 mechanisms used by DNSSEC.

2.4.4 ICANN gTLD related activity

See section 4.1.

3 Area: IP and Routing

In order to increase the security and maintain the stability of the global routing system, NLnet Labs contributes to the understanding of its dynamics both in terms of technology as well as its operation. In addition, we put effort in the development of tools and practices that lower the barriers to the deployment of security features.

NLnet Labs role is unique in the sense that Labs is neither vendor, nor operator and takes an inter-operator global perspective.

3.1 Inter-domain Routing Security and Stability

3.1.1 Extendible Next Generation Routing Information Toolkit (ENGRIT)

Goal

Design and development of a next generation Internet routing registry (IRR) toolset to decrease the costs of implementing and operating security practices.

Activities

In 2014, Per Bilse was contracted as a consultant to work on the Extendible Next Generation Routing Information Toolset project (ENGRIT). This toolset is being developed in collaboration with a few industry partners who form an advisory board to provide feedback on the design and implementation.

In the first phase of the project, we explored the requirements and first design of a new routing policy specification language to supersede the existing language RPSL. Together with our partners, the specification of the Routing Documentation Language (RDL) took shape. The goal of the new RDL language is to be more expressive, easier to use and read, and fits well with current practices in routing configuration and management.

After some iterations, Per Bilse implemented a compiler/translator for the RDL language. The specification is translated to router configurations in an AS, depending on their attributes, e.g. geolocation, topological characteristics, etc. RDL is only one part of the full ENGRIT toolchain that is envisioned to be a valuable tool for router configuration and management.

Results

In 2014 the RDL specification language has been presented at the UKNOF 28, IEPG (at the IETF 89), and RIPE 68 meetings. At the IETF 89 we organized a Bar BoF to discuss RDL with a number of routing experts. A first prototype of the RDL language compiler have been implemented.

Expected Impact

There is clearly an interest from the industry in a toolset that can assist in providing easier automation of routing configuration tasks and the ability to incorporate cryptographically signed resource information, thereby improving stability and security of the global Internet routing system. In particular, small and medium-sized networks can profit from a good open source toolset, as these networks are typical in between manual configuration (very small networks) and proprietary, in-house developed tools (for large networks with sufficient NOC staffing).

3.1.2 Self-managing Anycast Networks for the DNS (SAND)

Goal

This project proposal focuses on solutions for dynamic DNS anycast services to deal with changes in Internet connectivity, DNS query traffic, and other factors influencing their service in terms of availability, performance, and possibly security. And while optimizing for these quality of service terms, the operational costs have to be considered also. To achieve these operational performance and cost goals, we believe an automated management system potentially offers the best possible course of action.

SIDN Labs and NLnet Labs support this project with funding for an academic postdoc at the Universiteit Twente. Other industry partners are RIPE NCC, Netnod and SURFnet.

Activities

Ricardo Schmidt started in December 2014 as a postdoc at the Universiteit Twente for a period of two years funded by NLnet Labs and SIDN Labs. The first task will be the design and implementation of a monitoring infrastructure required for the self-management system using the monitoring-analysis-planning-execution feedback loop.

The project will be executed in close collaboration with NLnet Labs and SIDN Labs

Expected Impact

The result of the project reduces the complexity of managing a DNS anycast infrastructure, and provides flexibility and adaptability to act upon changes in the network and DNS client behavior (flash crowd, DDoS, etc.). In its operation, the system can also reduce operational costs: it is not only adding or moving anycast nodes, but if usage patterns indicate that certain nodes can be shutdown, this can reduce costs while performance metrics are still within specified bounds.

3.1.3 BGP Route Leaks Analysis

Goal

Study and get insight in the occurrence of BGP route leaks. New routing security enhancements proposed in the IETF SIDR WG do not touch upon the problems of route leaks. For discussion and solutions, a better understanding in the frequency and extent of route leaks is necessary.

Activities

In a pilot project, Stella Vouteva (BSc student intern) realized a prototype implementation for BGP route leaks detection. Benjamin Wijchers (MSc student) continued the project in 2014, first by reevaluate the findings of the pilot project, and rethink the detection and design of the analysis parts of the system. A full implementation is available that stores analyzed results for a month (due to disk usage, thus can be extended with the availability of huge database stores). Long-term statistics can be generated and stored in the database for trend analysis over periods of years or even decades.

Results

Implementation of a BGP routing analysis framework and an MSc thesis. Presentation at the RIPE 69 Routing WG.

Impact

Create better understanding of the problem, its frequency and extent—this can be important input for discussions on routing infrastructure security. Talents/students being trained in fundamental Internet architecture.

3.2 Inter-domain Routing Complexity

3.2.1 BGP Simulation

Goal

In the past years, we used our BGPSIM environment to study stability, resiliency, and stability properties of the Internet inter-domain routing system. Fundamental to this work is analysis of the complexity of the Internet routing infrastructure. We continue to work on this topic in collaboration with MSc students.

Activities

Jeffrey de Looff used our simulation lab to study the network complexity of our routing infrastructure, focusing on how small changes in the network could affect the global behavior of the network. Examples are analyzing the impact of failures at tier 1, tier 2, and tier 3 networks, by measuring the number of updates (announcements or withdrawals) that are the result of a failing link or AS network.

Results

Publication of an MSc thesis.

Impact

Increased understanding of the stability of the routing system and talents/students being trained in fundamental Internet architecture.

3.2.2 Analysis of BGP Evolution

Goal

The size of the global routing table grows at a faster rate than the amount of update messages being sent per day. In this study, we investigate the different components which together form the actual update message signal and examine the cause of the invariable signal of BGP background noise over the past decade

Activities

Tim Blankers analyzed the BGP routing infrastructure trends from 2005 to 2013. For example the growth in number of routing prefixes and routes, and a categorization of more active prefixes and networks (ASes) that contribute more to (dominate) the measured averages. Over the time period 2005 to 2013, patterns have been analyzed to find explanations for the observed statistics.

Results

Publication of an Msc thesis.

Impact

As with previous MSc project described in Section 3.2.1, increased understanding of the stability of the routing system and talents/students being trained in fundamental Internet architecture.

3.3 Other Projects

3.3.1 Open Data Analysis Related to National-Centric Critical Infrastructures

Goal

A concern with the release of government and private sector data is that sensitive information can be obtained by means of visualization techniques. The project uses a method of visual analytics known as feedback loop process to acquire insights from data.

Activities

Renato Fontana (MSc student intern) accomplished a proof-of-concept study to show the potential of analysis of public data and the identification of vulnerabilities in critical infrastructure. In this study, a national-level analysis of communication antennas, power plants, data centers locations was performed and visualized. A more detailed study on city-level complemented the study, covering power plants and energy consumption per zip code area. Location of data centers could be clearly determined by using visualization techniques.

Results

Proof-of-concept implementation of framework to access public data, analyze, and visualize relations. Publication of research report for MSc graduation.

Impact

Create some sense of apprehension of potential risks with publishing (public) data. Talents/students being trained in fundamental Internet architecture.

3.3.2 The Atlas Continuous Measurement Framework

Goal

The objective of this project is to design and implement a framework that will continually reproduce certain types of measurements in order to monitor certain network properties consistently.

Activities

Warwick Louw (BSc student intern) designed and implemented a framework to run and store RIPE Atlas measurements. The framework facilitates repeated experiments executed over different time periods and store results. Results are stored as network properties determined by interdependent measurements. Network properties can be properties such as DNS capability over an IPv6 network and which of those are DNSSEC capable. Results of the interdependent measurements are stored in a database.

Results

Implementation of the framework. Publication of BSc thesis.

Impact

The framework is used intern at NLnet Labs for path MTU measurements and its effect on DNSSEC. Talents/students being trained in fundamental Internet architecture.

4 Area: Knowledge Dissemination, Outreach, and/or Community Participation

NLnet Labs and its research engineers and software developers actively participate in areas where technology, governance, and public interest intersect with each other. NLnet Labs' staff volunteers in various community supporting positions.

4.1 ICANN

Akkerhuis is member of the Security and Stability Advisory Committee (SSAC) and is in 2014 appointed to the Root Server System Advisory Committee (RSSAC) Caucus[4].

4-https://www.icann.org/resources/pages/rssac-caucus-2014-05-06-en

Akkerhuis is appointed by the SSAC as a member of the Cross Community Working Group (CWG)[5]. ICANN proposed the creation of an IANA Stewardship Transition Coordination Group (ICG) “responsible for preparing a transition proposal reflecting the differing needs of the various affected parties of the IANA functions.” The CWG was formed as an integral part of this transition process, and to develop a proposal for the elements of the IANA Stewardship Transition that directly affect the naming community.

Akkerhuis acts as a liaison for ICANN in the ISO Technical Committee 46, 3166/MA meeting. (ISO 3166 is the International Standard for country codes and codes for their subdivisions.)

Finally Akkerhuis and Kolkman continue active participation in the ICANN preparation meetings hosted by EZ.

4.2 RIPE / Network Operations Community

NLnet Labs staff actively participates in the RIPE and broader operators community

Overeinder is vice-chair of the RIPE Program Committee and co-chair of the RIPE BCOP Task Force. Akkerhuis is a co-chair of the DNS-WG and since December 2013 Akkerhuis is a member of the ENOG program committee.

During RIPE68 and RIPE69 NLnet Labs’ staff disseminated its knowledge and expertise with a number of high impact appearances. See also Section 7.

Overeinder presented on Internet infrastructure security and mitigation strategies at a RIPE NCC regional meeting in Almaty, Kazakhstan and at the Holland Strikes Back Symposium[6].

4.3 IETF and Technical Community

Kolkman acts as chair of the WEIRDs WG and contributes to the timely specification of a Registration Data Access Protocol.

Kolkman is also active in an IAB program that advises the IAB on the strategy with respect to the IANA function within that context he participated in I* leadership meetings and is the principal author of “*A Framework for the Evolution of the Internet Assigned Numbers Authority(IANA)*”[7]

Wijngaards contributed to a BoF session at the IETF 89 discussing the issues on DNS and privacy. For discussion and exploring the design space, Wijngaards and Wiley submitted a draft document for consideration by the community, see also Section 7.

4.4 Global Internet Governance

End of 2013, Kolkman joined the *Panel on Global Internet Cooperation and Governance Mechanisms*. The panel is a diverse group of global stakeholders from government, civil society, the private sector, the technical community and international organizations—all deeply devoted to the future evolution of the Internet.

5-https://community.icann.org/display/gnsocwgdtstwrdshp/CWG+to+Develop+an+IANA+Stewardship+Transition+Proposal+on+Naming+Related+Functions

6-https://www.ripe.net/participate/meetings/regional-meetings/ripe-ncc-regional-meeting-almaty and http://www.hollandstrikesback.nl/

7-http://tools.ietf.org/html/draft-iab-iana-framework-02

From December 2013 to May 2014, the panel held meetings at three occasions, resulting in a report with key recommendations on how to evolve the Internet governance (IG) ecosystem to accommodate global needs for collaboration, interconnectivity and Internet growth.[8] The report also presents a roadmap and timeline for the future management of the Internet.

At the 5th Russian Internet Governance Forum (RIGF-2014), the Internet Merits award was presented to Kolkman.

At the NL IGF Event 2014, Kolkman and others organized a workshop “Nederland en de toekomst van internet”. In this workshop the results of the NETmundial were discussed and their implications to the Netherlands[9].

4.5 Other

Besides facilitating internships and research projects at NLnet Labs for BSc and MSc students, the staff gives colloquia and assists with practicums at the University of Amsterdam. The topics are inter-domain routing, DNS, and multi-path routing (layer 2: TRILL and SPB, layer 4: Multipath TCP, and layer 7: Multipath BGP).

In 2014, we attended/participated in a number of hackathons to discuss code with developers, and to reach out and help the adoption of our code in third party software or operating system distributions. The hackathons we took part in were: The Next Web 2014 hackathon, Amsterdam (getdns API); OpenBSD 2014 hackathon Ljubljana, Slovenia (Unbound); and EuroBSDCon 2014, Sofia, Bulgaria (Unbound).

Kolkman was member of the program and prize committee for the Workshop on Root Causes and Mitigation of Name Collisions (WPNC14, http://namecollisions.net).

8-http://internetgovernancepanel.org/panel-report

9-https://ecp.nl/actueel/4145/nl-igf-event-een-smeltkroes-van-ideea-laquo-n-wensen-en-aanbevelingen.html

5 Area: NLnet Labs Continuity

5.1 Strategic plan

During 2013 we reviewed NLnet Labs mission, vision and strategy and, for the first time, published a Strategic Plan[10]. The document emphasizes our mission "*To provide globally recognized innovations and expertise for those technologies that turn a network of networks into an Open Internet for All.*" Further, it describes how our mission relates to our statutes and the principles for setting direction. The strategy plan also discusses the directions in which we plan to develop over the coming years, and our ideas to secure financial continuity.

In 2nd half of 2015, we will update and extend our Strategic Plan for the next period of two to three years.

5.2 Open Netlabs BV

NLnet Labs is diversifying its income by identifying and engaging with more parties to provide a continued commitment to fund its work and by cooperating with a wholly owned subsidiary: Open Netlabs BV.

Open Netlabs BV operated in 2014 as the commercial vehicle supporting the open source activities by securing sustainable income on the longer term. Since the start in 2013 and continued in 2014, the positioning and promotion of the activities are made known and discussed during events like ICANN, IETF, and RIPE meetings. Besides the initial focus on providing Unbound support and (limited) training and consultancy, we extended our offerings with NSD and OpenDNSSEC support. Adjusting and expanding strategy and portfolio will be a running process.

Han Brouwers is the director of Open Netlabs BV. Stichting NLnet Labs owns 100% of the Open Netlabs BV stock.

[10] -http://www.nlnetlabs.nl/labs/about/Strategic-Plan.pdf

6 NLnet Labs organization and finance

6.1 Board

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its board consists of three to five members with staggered terms. The board's composition and most recent rotation schedule is shown in the tables.

Six board meetings took place in the year 2014. Olaf Kolkman participated in the board meetings in his role of Director of NLnet Labs for the first half year of 2014. Benno Overeinder participated as director of NLnet Labs for the second half year of 2014. Han Brouwers participated as the director of Open Netlabs B.V.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€177 for 2014). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

NLnet Labs Board in 2014

name	function	end of term
Frances Brazier	secretary	December 28, 2017
Roelof Meijer	member	May 31, 2015
Wytze van der Raay	treasurer	December 28, 2016
Leo Willems	chair	February 1, 2016
Ted Lindgreen	member	January 31, 2018

Director and Board Member Additional Functions in 2014

Frances Brazier	Ted Lindgreen	Roelof Meijer	Wytze van der Raay	Leo Willems	Olaf Kolkman/ Benno Overeinder
- Professor Engineering Systems Foundations at *the Technische Universiteit Delft (TU Delft)* - Chair of the board of *Landelijk Netwerk Vrouwelijke Hoog leraren (LNVH)* - Member of the supervisory board of *Kennisnet*	none	- CEO of *SIDN* - Participant in *Platform Internet Veiligheid* - Participant in *Programmaraad Digivaardig & Digiveilig* - Chair *Digiveilig* - Member of the Council of the Board of *PI Lab* - Council member of *the ICANN ccNSO* - Participant in the *IGF* - Member of the advisory council of *Dutch ISOC Chapter*	- Team leader *CAcert critical system administrators* - Administrator, *Stichting Wereldwinkel Doorn*	- Owner TUNIX Digital Security. Member of the board of *Stichting IT Projecten (StitPro)*.	See page 23

6.2 Staff

NLnet Labs employed eight people in 2014: Jaap Akkerhuis, Olaf Kolkman (director until June 2014), Wouter Wijngaards, Benno Overeinder (director from July 2014), Matthijs Mekking (until July 2014), Willem Toorop, Yuri Schaeffer, Ralph Dolmans. and Berry van Halderen (as of December 2014). The director of Stichting NLnet Labs is responsible for the daily management of all activities of the laboratory, including development of strategies and plans for new activities.

Director Olaf Kolkman accepted the assignment at Internet Society (ISOC) as Chief Internet Technology Officer as of July 2014.

Matthijs Mekking accepted a position at Dyn corporation as of August 2014.

The open positions at NLnet Labs were filled in by Berry van Halderen (December 2014) and Hoda Rohani (January 2015).

Finances are administered by Patricia Otter of the Stichting NLnet.

6.3 Offices

NLnet Labs resided at the Amsterdam Science Park ever since its incubation in 1999. Its offices are located in the Matrix II building.

6.4 Finances

NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in April 2015, these are the unaudited numbers[11].

Stichting NLnet Labs primarily finances its projects and activities from grants obtained from two organizations:

1. Stichting NLnet: The long term financial commitment of NLnet towards NLnet labs has been codified in a subsidy contract since 2007. In 2010 NLnet Labs was given notice that because of uncertainty of available funding, that contract is terminated as of Jan 1, 2016.
2. SIDN, the Internet domain registry for the Netherlands: A subsidy contract between SIDN and NLnet Labs provides for structural financing for the period Jan 1, 2012 – December 31, 2016.

A second means of income are subsidies and donations by other parties. NLnet Labs has developed a sponsor agreement. For 2014, we would like to acknowledge Verisign, Comcast, AFNIC, DK Hostmaster A/S, SWITCH, and NIC.AT for their continued generous support.

In addition, income may be obtained by providing consultancy or subsidized research on Internet architecture, governance, and technology issues and by providing Open Source programming services to third parties. Our activities in these areas are reported above.

Finally Unbound, NSD, and OpenDNSSEC support contracts via Open Netlabs B.V. are sources of additional income in 2014.

[11] 11-Audited finances can be found in “Kengetallen jaarrekening 2014” as published on http://www.nlnetlabs.nl/labs/about/

6.5 Fiscal Status

On 20 September 2007, NLnet Labs has been recognized as an institution with general benefit objectives, “Algemeen Nut Beogende Instelling (ANBI)”. This status has become relevant under new regulations that are effective as of January 1, 2008.

6.5.1 Income in 2014

At the end of 2013, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2014, with a total of 780 k€. Based on this budget and the expected consultancy income, 336.8 k€ grants were requested from SIDN and Stichting NLnet. Both sponsors allocated these funds for 2014, to be received by NLnet Labs on a quarterly basis.

Stichting NLnet & Stichting SIDN

are NLnet Labs’ major benefactors.

In addition to these regular subsidies Stichting NLnet awarded a subsidy of 132 k€ in order to perform business development within the context of the Open Netlabs B.V. These funds were immediately allocated towards a special fund for business development, henceforth they appear on the balance sheet.

Regular sources of non-subsidy income are the NSD and Unbound support contracts and a consultancy contract with ICANN (mostly ISO3166 related work) and a compensation for the bandwidth used by the secondary server for .PT.

In addition NLnet Labs received significant donations from Comcast, Verisign, Afnic, DK Hostmaster A/S, SWITCH, and NIC.AT amounting to a total of 120 k€ income above budget.

IIS (the Internet Foundation in Sweden) and CIRA (.CA registry) generously donated funds for the continued development of OpenDNSSEC.

Interest received amounted to 14 k€

Finally NLnet Labs payed an advance for the staff and other costs incurred for the Open Netlabs BV; these costs (21 k€) were immediately recovered from Open Netlabs BV and are not shown in the tables.

The following organizations are acknowledged for their generous contributions

6.5.2 Expenditure in 2014

The major expenditure categories of NLnet Labs in 2014 are staff, travel and housing. In July and August there were mutations, reducing our staff from 8 persons (7.7 FTE) to 6 persons (5.8 FTE). In December we expanded our 6 person staff to 7 persons (6.7 FTE). The total expenditure on staffing in 2014 is 542 k€. Housing and travel make up for another 111 k€ out of the total of 727 k€ expenditure.

As in 2013, we made in 2014 an earmarked reservation of 132 k€ for Open Netlabs business development. From the ENGRIT designated reservation of 135 k€ at the start of 2014, we withdraw 21 k€ to contract an expert.

After making these reservations and valuations NLnet Labs had a negative result of € 4,992. The general financial reserve at the end of 2014 is 64k€.

Balance Sheet (k€)

Assets		**Liabilities**	
Inventory	2	**General Reserve**	64
Open Netlabs BV stock and loans	63		
Receivables	25	**Open Netlabs BV Business Development Fund**	264
Bank & Cash	564	**Reservation ENGRIT**	114
		Reservation SAND	145
		Accounts Payable	11
		Tax and Social Premium Payable	18
		Other liabilities	37
Total	654		654

Income

	2013 actual (k€)	2014 actual (k€)	2014 budget (k€)	2015 budget (k€)
NLnet Subsidy	286	337	337	359
SIDN Subsidy	286	337	337	359
Other Donations	209	130	9	36
Consultancy and other Income	107	17	17	17
NSD & Unbound Support	80	67	79	0
Interest Income	3	14	2	2
Sub Total	972	902	780	772
Business Development Subsidy from NLnet	132	132	132	66
Total	1,104	1,034	912	838

Expenditure

	2013 actual (k€)	2014 actual (k€)	2014 Budget (k€)	2015 Budget (k€)
Staff	564	542	615	590
Housing	44	56	55	57
Travel	45	55	64	67
Depreciation	2	2	5	5
ENGRIT Project Costs	3	21	0	0
Other costs	33	51	46	52
Sub Total	691	727	780	772
Negative Result Open Netlabs	1	201	0	0
Project Reservation NLnet Business Development	132	132	132	66
Project Reservation ENGRIT	135	-21	0	0
Project Reservation SAND	145	0	0	0
Total	1,104	1,039	912	838

6.5.3 Budget for 2015

The 2015 budget has been drawn up on 30 September 2014. Based on having 7.6 FTE we have budgeted a total expenditure of 772k€

On January 20, 2012 Stichting SIDN signed a five year contractual commitment to subsidize 50% of the expenditure needed to execute our chartered activities. For 2015, SIDN will cover 359 k€ in four quarterly grants of almost 90 k€. Stichting NLnet will subsidize our activities with 337 k€, paid in four quarterly grants of 84 k€.

Additionally, NLnet Labs expects to receive about 17 k€ from consulting activities and 36 k€ through donations.

6.5.4 Financial Outlook

In December 2010, Stichting NLnet has formally announced that it will terminate its subsidy contract by January 1, 2016, due to an expected lack of funds by that time. Director and board have started an effort to identify new sponsors and other sources of income with the goal of establishing a solid base for continued existence of NLnet Labs beyond the expiration of this subsidy contract.

In January 2013 Han Brouwers joined NLnet Labs as business developer. Stichting NLnet intended to subsidize this initiative, as of 2013, for 3 years. In 2013 and 2014, 132 k€ was immediately allocated towards a special fund for business development. For 2015, the last installment of 66 k€ is allocated covering for the activities of the business developer for a half year.

The business development is part of the activities of Open Netlabs BV, see also Section 5.2 for details.

7 Publications, Presentations and reports

Publications

- RFC7127: "***Characterization of Proposed Standards***", Kolkman, Bradner, and Turner, January 2014, https://tools.ietf.org/html/rfc7127
- RFC7129: "***Authenticated Denial of Existence in the DNS***", Gieben and Mekking, February 2014, https://tools.ietf.org/html/rfc7129
- SAC064: "***SSAC Advisory on Search List Processing***". Akkerhuis as contributing SSAC member, February 2014. https://www.icann.org/en/groups/ssac/documents/sac-064-en.pdf
- SAC065: "***SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure***", Akkerhuis as contributing SSAC member, February 2014. https://www.icann.org/en/groups/ssac/documents/sac-065-en.pdf
- SAC067: "***Overview and History of the IANA Functions***", Akkerhuis as contributing SSAC member, August 2014. https://www.icann.org/en/groups/ssac/documents/sac-067-en.pdf
- SAC068: "***SSAC Report on the IANA Functions Contract***", Akkerhuis as contributing SSAC member. October 2014. https://www.icann.org/en/groups/ssac/documents/sac-068-en.pdf
- RSSAC 002: "***Advisory on Measurements of the Root Server System***", Akkerhuis as contributing RSSAC Caucus member, November 2014. https://www.icann.org/en/system/files/files/rssac-002-measurements-root-20nov14-en.pdf
- SAC069: "***SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition***", Akkerhuis as contributing SSAC member. December 2014. https://www.icann.org/en/groups/ssac/documents/sac-069-en.pdf

Presentations

- "***Mapping the Dutch Critical IP Infrastructure***", Overeinder, NSCS-NL, Den Haag, The Netherlands, January 2014.
- "***Mapping the Dutch Critical IP Infrastructure***", Overeinder, Cisco SP Security Forum, Amsterdam, The Netherlands, February 2014.
- "***A programmatic approach to generating router configurations***", Bilse, IEPG Meeting, IETF 89, London, UK, March 2014. http://www.iepg.org/2014-03-02-ietf89/rdl-IEPG-89.pdf
- "***RIPE Atlas***", Jaap Akkerhuis, ccTLD Tech Day, ICANN 49, Singapore, SG, March 2014. https://singapore49.icann.org/en/schedule/mon-tech/presentation-ripe-atlas-24mar14-en.pdf
- "***Confidential DNS***", Wijngaards, Encryption of DNS requests for confidentiality (dnse) BoF, IETF 89, London, UK, March 2014. http://www.ietf.org/proceedings/89/slides/slides-89-dnse-2.pdf
- "***Introduction to RDL***", Bilse, UKNOF 28, Reading, UK, April 2014. https://indico.uknof.org.uk/materialDisplay.py?contribId=21&materialId=slides&confId=30
- "***Flexible DNSSEC Key Rollovers***", Mekking, Digital Security Lunch Colloquium, Faculty of Science, Radboud University, Nijmegen, The Netherlands, Friday, 27-04-2012. http://www.ru.nl/ds/about_ds/lunch_colloquium/
- "***getdns API Implementation***", Toorop, DNS-OARC Spring Workshop, Warsaw, Poland, May 2014. https://indico.dns-oarc.net/event/19/contribution/4/material/slides/0.pdf
- "***DNSSEC Audit Framework***", Mekking, DNS-OARC Spring Workshop, Warsaw, Poland, May 2014. https://indico.dns-oarc.net/event/19/contribution/29/material/slides/0.pdf
- "***getdns API implementation***", Toorop, Open Source WG, RIPE 68, Warsaw, Poland, May 2014. https://ripe68.ripe.net/presentations/268-getdns-API-Implementation.pdf
- "***Measuring the deployment of DNSSEC over the Internet***", Canceill, DNS WG, RIPE 68, Warsaw, Poland, May 2014. https://ripe68.ripe.net/presentations/232-slides.pdf
- "***RDL: A Programmatic Approach to Generating Router Configurations***", Overeinder, Routing WG, RIPE 68, Warsaw, Poland, May 2014. https://ripe68.ripe.net/presentations/366-ripe68-rdl-20140515.pdf

- "***DNSSEC Operational Practices for Authoritative Name Servers***", Mekking, BCOP TF, RIPE 68, Warsaw, Poland, May 2014. https://ripe68.ripe.net/presentations/214-ripe68-bcop-dnssec.pdf
- "***Infrastructure Attack Vectors and Mitigation***", Overeinder, RIPE NCC Regional Meeting, Almaty, Kazakhstan, June 2014. https://meetings.ripe.net/almaty2014/presentation-upload/show.php?id=15
- "***DNSSEC Audit Framework***", Mekking, 7th CENTR Security workshop (CENTR Jamboree 2014), Paris, France, June 2014. https://centr.org/system/files/agenda/attachment/secur7-mekking-dnssec_audit_framework-20140602.pdf
- "***Name Server Round Table***", Mekking and others, Tech Day, ICANN 50, London, UK, June 2014. https://london50.icann.org/en/schedule/mon-tech
- "***getdns API implementation***", Toorop, DNSSEC Workshop, ICANN 50, London, UK, June 2014. https://london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-getdns-api-25jun14-en.pdf
- "***Measuring DNSSEC Validating Resolvers Using RIPE ATLAS***", Toorop, DNSSEC Workshop, ICANN 50, London, UK, June 2014. https://london50.icann.org/en/schedule/wed-dnssec/presentation-dnssec-validation-deployment-25jun14-en.pdf
- "***DNSSEC Via a New Stub Resolver***", Toorop, OSCON2014, Portland, OR, July 2014. http://cdn.oreillystatic.com/en/assets/1/event/115/DNSSEC Via a New Stub Resolver Presentation.pdf
- "***DNS at NLnet Labs***", Jaap Akkerhuis, ccTLD Tech Day, ICANN 51, Los Angeles, US, October 2014. https://la51.icann.org/en/schedule/mon-tech/presentation-nlnet-labs-13oct14-en.pdf
- "***Developments in DNS and BGP Security***", Overeinder, Holland Strikes Back: Dutch Initiatives Against Cyber Attacks and Abuse, Amersfoort, The Netherlands, October 2014. http://www.slideshare.net/splend/hsb-secure-dns-en-bgp-ontwikkelingen-benno-overeinder
- "***Using the getdns API – a new application friendly interface to the DNS***", Toorop, Huque, Wiley and Dickinson, RIPE 69 tutorial, London, UK, November 2014. https://ripe69.ripe.net/programme/meeting-plan/tutorials/
- "***News About NSD 4.1***", Jaap Akkerhuis, Open Source WG, RIPE 69, London, UK, November 2014. https://ripe69.ripe.net/wp-content/uploads/presentations/69-NSD4.1-news.key.zip
- "***Quantitative Analysis of BGP Route Leaks***", Overeinder, Routing WG, RIPE 69, London, UK, November 2014. https://ripe69.ripe.net/wp-content/uploads/presentations/157-RIPE-69-Routing-WG.pdf

Work in Progress

- "***Minimal Incremental Zone Transfer in DNS***", Mekking and Gudmundsson, January 2014. https://tools.ietf.org/html/draft-mekking-mixfr-00
- "***Technical Considerations for Internet Service Blocking and Filtering***", Barnes, Cooper & Kolkman, January 2014, http://tools.ietf.org/html/draft-iab-filtering-considerations-06
- "***Confidential DNS***", Wijngaards and Wiley, March 2014. https://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-02.

Student Reports

In 2014 we had 6 interns. The following reports and thesis were published in 2014

- "***Securing the last mile of DNS with CGA-TSIG***", Buisman, MSc thesis, University of Amsterdam, January 2014. https://www.nlnetlabs.nl/downloads/publications/report-rp2-buijsman.pdf
- "***Structural Measurement and Tracking of Path MTU and Fragmentation Problems***", Louw, BSc thesis, January 2014.
- "***Open Data Analysis to Retrieve Sensitive Information Regarding National-Centric Critical Infrastructures***", Fontana, MSc thesis, University van Amsterdam, February 2014. http://www.nlnetlabs.nl/downloads/publications/RP45 Open Data Analysis - Critical infrastructures.pdf
- "***Measuring the deployment of DNSSEC over the Internet***", Canceill, MSc thesis, University of Amsterdam, July 2014. http://www.nlnetlabs.nl/downloads/publications/report-rp2-canceill.pdf

- "***BGP Evolution Analysis***", Blankers, MSc thesis, Vrije Universiteit Amsterdam, July 2014. http://www.nlnetlabs.nl/downloads/publications/msc-thesis-blankers.pdf

Student work in progress:

- Benjamin Wijchers worked on "***BGP Route Leaks***".

Blog Posts

- Does Open Data Reveal National Critical Infrastructures?, Fontana and Overeinder, February 2014. https://www.nlnetlabs.nl/blog/2014/02/21/open-data-and-critical-infrastructures/
- Hackathon at TNW-2014, Wijngaards and Kolkman, May 2014. https://www.nlnetlabs.nl/blog/2014/05/01/hackathon-at-tnw-2014/
- OpenDNSSEC project transferred to NLnet Labs, Overeinder, September 2014. https://www.nlnetlabs.nl/blog/2014/09/15/opendnssec-project-transferred-to-nlnet-labs/
- NSD 4.1: zonefile-mode and fork fix, Wijngaards, September 2014. https://www.nlnetlabs.nl/blog/2014/09/19/nsd-4-1-zonefile-mode-and-fork-fix/

NLnet Labs staff responsibilities

- **Akkerhuis**:
  - ICANN representative in the ISO 3166 Maintenance Agency
  - Member of the ICANN Security and Stability Advisory Council (SSAC)
  - Member of the ICANN Root Server System Advisory Committee (RSSAC) Caucus
  - Co-chair of the RIPE DNS working group.
  - RIPE Arbiter
  - Member of the ccNSO study group on Use of Names for Countries
- **Kolkman**:
  - Chair of the IETF WEIRDS working group
  - Chair of the IAB IANA evolution program.
  - IAB/IETF representative in the EU Multi-Stakeholder Platform on ICT Standardization
  - RIPE Arbiter
  - Member of the Panel on Global Internet Cooperation and Governance Mechanisms
  - Member of the program committee for the Workshop and Prize on Root Causes and Mitigation of Name Collisions 2014 (WPNC14)
- **Overeinder**:
  - Vice-chair of the RIPE Program Committee
  - Co-chair of the RIPE Best Current Operational Practices Task Force
  - Member of the ENISA Internet Infrastructure Security and Resilience Reverence Group

Stichting NLnet Labs

Science Park 400, 1098 XH Amsterdam

e-mail: labs@nlnetlabs.nl, *web*: http://www.nlnetlabs.nl/