Annual Report 2010

Colophon

This document was prepared with LibreOffice software using the OpenDocument file format. The front page, NSD, and Unbound logo were created using Blender.
Typeface: Helvetica Neue and Gill Sans.

NLnet Labs Document 2011-001

We are happy to present NLnet Labs Annual report 2010. It is intended to present an overview of Labs' various activities to those who support NLnet Labs financially, through grants or support contracts, and for those who have shown a general interest in our activities. The first half of this report presents an overview of our activities, while the second half presents details about the organizational and financial aspects of the NLnet Labs foundation.

1 NLnet Labs

The Internet's strength is that it allows people to connect and communicate with each other on the Internet without any concern for the infrastructure between end-nodes. This allows people to publish, provide services, to purchase, read, and consume in a global and truly free manner. The availability of open source and open standards is one of the success factors for protocols being deployed on the Internet (RFC5218).

NLnet Labs is a research and development group that focuses on developments in Internet technology, where public interest is often more pressing than commercial interest. Our activities can best be described as contributions that bridge the gap between theoretical insights and practical deployments, that bridge between technology and policy, and that are rooted in engineering and standardization. It is our goal to contribute to the public interest by playing an active and important role in the development of open source software, participating in the development of open standards, and disseminating knowledge through training, consultancy, and *evangineering*. NLnet Labs is recognized for its expertise in Internet system technology and architecture, in particular in DNS and DNSSEC. NLnet Labs' software is an important component of the Internet infrastructure. NLnet Labs plays a significant role in standards development. Dissemination of knowledge is realized through education and collaboration.

Stichting NLnet Labs was founded in 1999 by Stichting NLnet. The budget of NLnet Labs, a non-profit organization, is mainly based on a subsidy from Stichting NLnet. Stichting NLnet has provided a long-term commitment in the form of a subsidy contract such that NLnet Labs can guarantee support for the software it develops.

The NLnet Labs offices are located in the Amsterdam Science Park (ASP).

2 Area of Interest: DNS and DNSSEC

Signing the Root

July 16, 2010 the DNS root was signed with key material that was generated during a key ceremony in Culpeper VA on June 16, 2010.

The key ceremony is designed to provide a secure and tamper proof environment and procedure for the generation of the private keys used to sign the root. The procedure calls for 7 Crypto officers of which at least 3 have to be present to access a Hardware Signing Machine on which the private keys are stored.

Contrary to some reports the Crypto Officers do not hold the key to the Internet but only a physical key that provides access to a smart card that is stored in a safe behind multiple tiers physical security.

NLnet Labs' director Olaf Kolkman is entrusted as one of the crypto officers.

2.1.1 DNSSEC Evangineering

NLnet Labs believes that deployment of DNSSEC, a security extension to one of the protocols that is essential to the operation of the Internet, is the most important area where NLnet Labs can make a significant difference. We contribute to global deployment by providing tools and software such as NSD, Unbound, ldns, Net::DNS and OpenDNSSEC. But we also contribute by providing technical information, teaching courses, and popularizing the technology. The combination of solid engineering combined with *spreading the word* on the necessity of the technology is what we have come to call 'evangineering'.

In 2010 DNSSEC was deployed in the root zone and several top-level domains (TLD), including the Dutch .NL zone. By the end of 2010 about 50 TLDs were DNSSEC signed and their number continues to grow. In 2011 .COM will be DNSSEC signed and various registrars offer DNSSEC interfaces.

NLnet Labs' persistent efforts have played a continuing role in these developments.

2.1.2 The Unbound Recursive Nameserver

Unbound is a validating caching resolver implementation with full DNSSEC support. It was written over the course of 2007 in order to provide a free and open source reference implementation of the DNSSEC protocol suite. The 1.0 version was released on May 20, 2008. Unbound is now present in many BSD port distributions and Linux package repositories.

The Unbound implementation in C is based on the Unbound Java implementation developed by Verisign, Nominet, and Kirei. The modular, clean design and some parts of the state machine were reused. The C code was written with performance in mind. This means the same lean and mean attitude from NSD, but since this is a resolver, many more features are necessary.

In 2010 the Unbound versions 1.4.2 to 1.4.7 have been released. Major new feature is prefetching, implemented in such a way that making popular names readily available from cache comes with a penalty of no more than 10% extra CPU and bandwidth. Support for the ECC-GOST crypto algorithm has been added. We also added unbound-anchor, a tool to create a root anchor file and keep it up to date. In version 1.4.3 an error that could under special circumstances cause a remotely triggered denial of service was fixed.

Unbound is targeted for ISP and Enterprise environments. NLnet Labs is currently not in the position to offer 1st and 2nd line support but collaborates with parties such as Men and Mice whose employees were trained and who have a 3rd line support contract with NLnet Labs.

Unbound is available at the dedicated website http://unbound.net, hosted and maintained by NLnet Labs.

2.1.3 The NSD Authoritative Nameserver

The NLnet Labs Name Server Daemon (NSD) is an authoritative RFC compliant DNS name server. It was first conceived to allow for more genetic diversity for DNS server implementations used by the root-server system. NSD has been developed for operations in environments where speed, reliability, stability, and security are of high importance. NSD is currently used on some root servers such as the L and K root- servers. It is also in use by several top-level domain registries such as .NL, .DE, .BR, .SE, and .UK.

NSD is considered quite stable and can be found in almost all software repositories. We have released three new patch versions of NSD. Version 3.2.4 introduced some new configure options to tune TCP traffic. This work was done in order to prepare NSD for a signed root and the expected increase in TCP queries. Besides that, DLV support was added. From version 3.2.5 and up, users are able to specify the DNS Name Server Identifier Option (NSID, RFC 5001). Version 3.2.6 fixed an important bug regarding NSEC.

NLnet Labs commits to long term support of NSD. Not only will it announce the termination of support two years in advance, it also offers support contracts in 3 varieties.

2.1.4 Port Maintenance

We maintain the FreeBSD ports of software products we develop. This allows us to get a good handle on completeness of the installation instructions. Besides it provides insight on the availability of, and dependencies on a typical installation environment. We do not maintain ports and equivalent distribution mechanisms (such as RPM and DEB packages) for other operating systems.

2.1.5 OpenDNSSEC: A DNSSEC Turnkey Solution

OpenDNSSEC is a collaborative project, which NLnet Labs has joined in 2008. The goal is to create a product that will handle zone signing and key management, and can be easily integrated in existing DNS deployments. The software consists of two core modules, called the enforcer and the signer. The enforcer implements DNSSEC policies and handles key management. The signer takes care of continuous (re-)signing. The development of the OpenDNSSEC signer is in hands of NLnet Labs. The signer module is implemented in a combination of the Python and C languages. OpenDNSSEC 1.0.0 was released in February 2010. This very first release obviously revealed initial bugs, as well as some performance problems. These issues were resolved in version 1.1.0, which was released in May 2010. It evolved to version 1.1.3 (released in September 2010).

A current critique on OpenDNSSEC is the extensive list of software dependencies required by the product. This motivated NLnet Labs to develop a C-based version of the OpenDNSSEC signer, dropping all the Python related dependencies. This decreases the number of dependencies. Also, the new signer module is designed for incremental signing, making it possible to support IXFR and Dynamic Update in the future. These developments are part of version 1.2.0, which saw a release candidate at the end of 2010.

Known users of OpenDNSSEC are SURFnet, CAcert, ICANN, as well as some top-level domain registries including .NL, .SE, .UK, .DK, .FI, .FR, and .LU.

OpenDNSSEC is distributed under a BSD license. For more information, see the website at http://www.OpenDNSSEC.org.

2.1.6 The ldns Software Library

Ldns is a C library aimed to simplify DNS programming. It allows developers to easily create software conforming to current RFCs and Internet Drafts. The library originates from the Drill tool, which was written to aid in DNSSEC debugging. Since drill needs a nearly complete DNS library to do its work, it was chosen to focus on the library itself, and make drill a part of that project. It was also influenced by the Perl Net::DNS library.

Interest in and usage of ldns has been steadily increasing over the years, most likely because of increasing world-wide interest in DNSSEC deployment. OpenDNSSEC depends heavily on ldns and so does Dan Kaminsky's Phreebird tool. Ldns is included in the software repositories of several operating systems, among which Fedora, Debian, Ubuntu, and FreeBSD.

Ldns is currently in maintenance mode, so only patch releases were made. In 2010, quite a few bugs were found in the library. This shows that ldns is actually in use to a substantive degree. Most reports were about the ldns resolver, memory usage, and reading and writing records. This resulted in four releases, 1.6.4 to 1.6.7, resolving the issues. Other noticable contributions to the ldns library are pyldns and NETLDNS, the Python and .NET port of ldns, and the implementation of new DNSSEC algorithms GOST and ECDSA (the latter being experimental).

Ldns is distributed under a BSD license.

2.1.7 The Perl Net::DNS and Net::DNS::SEC Libraries

The maintenance responsibility for the Perl libraries Net::DNS and Net::DNS::SEC is a task that NLnet Labs started in 2005. In 2010 Net::DNS::SEC saw one maintenance releases. Net::DNS and Net::DNS::SEC are published through CPAN and via the www.net-dns.org website.

2.2 DNSSEC Training and documentation

In 2010 we presented various DNSSEC lectures and tutorials varying from 30 minute overview presentations to 3 day in-depth workshops. The 3 day training intends to provide participants sufficient background and practice to feel comfortable to deploy DNSSEC in their own environment. The DNSSEC Howto is an integral piece of the course material. That document is maintained at NLnet Labs. The Howto can be downloaded from the NLnet Labs website at http://www.nlnetlabs.nl/dnssec_howto/.

2.3 DNS Communities and Community building

2.3.1 Integrating Testing And Learning of Interface Automata

NLnet Labs decided to become a user committee member in the research project 'Integrating Testing And Learning of Interface Automata' (ITALIA). This research, proposed by the Radboud University Nijmegen, deals with the design of algorithms that will allow computers to learn complex state diagrams by providing inputs and observing outputs. The research objective of the ITALIA project is to further develop this technique and to construct a tool set that will allow us to learn, routinely and fully automatically, state machine models with up to 40 state variables. The project is unique in bringing together research on automata learning with research on machine learning, model based testing, game theory and computer-aided verification.

DNS(SEC) is considered to be a system whose normal behavior is deterministic, but which may exhibit nondeterministic behavior due to exceptions, and is therefore to be considered an ideal system for this research. As a user committee member, we provide help with this specific case study.

2.3.2 CENTR, OARC, and the DNSSEC Industry Coalition

NLnet Labs has observer status in the Council of European Top Level Domain Registries (CENTR), is a member of OARC, the DNS Operations, Analysis, and Research Center (OARC), and a member of the DNSSEC Industry coalition. This latter is a industry consortium promoting and expediting the implementation of DNSSSEC. Details about this can be found at http://dnsseccoalition.org/website/.

2.3.3 DNSSEC.nl

The DNSSEC.nl platform, formed in 2009, is aimed at finding solutions for open issues that are blocking widespread DNSSEC deployment in the Netherlands. The platform focuses on DNSSEC deployment for the .nl ccTLD, the Dutch (ISP) market, under Dutch law and for the Dutch local Internet community as stakeholders. Of course we hope that the solutions and discussions that this platform produces can serve as a guideline for implementations in other parts of the world. Its charter can be found at http://www.dnssec.nl/dnssec-nl-platform-charter/

NLnet Labs is one of the organizations that supports the platform.

2.3.4 The Kyoto DNS Security, Stability and Resiliency symposium

Kolkman was a member of the program committee of the symposium that was centered around measuring the DNS' health.[1]

3 Area of Interest: Routing and Addressing

The activities for 2010 in inter-domain routing can be categorized in BGP modeling and simulation, and in BGP routing security. Activities in the IRTF Routing Research Group (RRG) ended with the IETF in March 2010: the RRG concluded its activities, conform its charter.

The BGP modeling and simulation project continued in 2010 with a study to analyze the influence of Internet topology (actually AS topology) on BGP performance. Shaza Hanif, a MSc. student from the VU University Amsterdam, worked for 6 months on this project. For this study, the BGP simulator developed by Maciek Wojciechowksi was used. For the baseline study, recent AS topologies were obtained from the CAIDA repository and experiments with BGP beacons and monitors were repeated. From these experiments, the BGP convergence time distributions were calculated. To study the influence of AS topologies on the BGP performance (measured by BGP convergence), we obtained a topology generator from Simula Research Laboratory[2]. With this tool, we can generate different AS topologies with certain characteristics, e.g., a flat or hierarchical (tree-like) Internet topology, or a tier 1 and large tier 2 clique topology, and many topologies in between and for different topology sizes. This study includes many dimensions of freedom—parameters to vary—and only a small subset of all possible scenarios have been studied. Despite this fact, we have obtained interesting results that are reported in Shaza Hanif's MSc. thesis.

1 Report at: http://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf
2 http://simula.no/

A full-day meeting with Geoff Huston and George Michaelson from APNIC generated new ideas for studies with the BGP simulator, e.g., the influence of routing security technologies on BGP operations, or why is the background “noise” in the BGP control plane constant while the Internet has grown spectacularly in the past 10 years. We can test various hypotheses to explain these phenomena to test their validity, i.e., the hypotheses’ ability to explain the observed behavior.

In November 2009, NLnet Labs and GNKS Consult successfully submitted a project proposal to ENISA on stocktaking of current routing security deployment. In January 2010 the project started with a kick-off meeting in Athens, Greece. The approach to stocktaking was of two kinds: an online questionnaire and one-on-one interviews with network operators and researchers. In the first month we prepared an online questionnaire and the questions for the interviews. The online questionnaire ran form March to half April 2010. To generate interest and seek support for the stocktaking activity, we presented our study at the LINX community meeting in London. The results of this part of the stocktaking was presented at a plenary session of the RIPE 60 meeting in Prague, Czech Republic. A panel discussion on the implications of the results was held during the Routing WG meeting at the same RIPE 60. The one-on-one interviews (in total 22) ran from February to beginning of May 2010. The results of the online survey and one-on-one interviews were brought together and analyzed, and finally resulted in an ENISA report[3]. The main conclusions of the report were presented at the IEPG meeting at the IETF 78 in Maastricht.

As a kind of spin-off of the ENISA study, NLnet Labs' involvement in RPKI became substantial in the second half of 2010. Resource PKI (RPKI) is a first step in securing the inter-domain routing infrastructure. RPKI is defined in a set of IETF Internet Drafts, now with the IESG for approval. An implementation of RPKI has been developed by a consortium (mainly by ISC, funded by DHS), and a testbed has been up and running since the beginning of 2010. In October 2010, we co-organized a RPKI workshop at the RIPE 61 meeting in Rome, Italy. During this workshop, NLnet Labs and SURFnet became part of the RPKI testbed. Resources of SURFnet were signed and Route Origin Authorisations were published, while the RPKI software runs on a NLnet Labs server. As an example, routers in Texas, US can validate the route announcements of address prefixes used by SURFnet. For next year, NLnet Labs and SURFnet will run a pilot project on RPKI deployment.

The ENISA routing security study and RPKI project generated some interest from a journalist of Computable magazine. The interview was published in January 2011.

4 Area of Interest: IPv6

NLnet Labs position is that the deployment of IPv6 is key to the preservation of an Internet that remains open for innovation, new consumers, and new market parties. Since its establishment in 1999 NLnet Labs has a strong interest in IPv6 and has delivered all of its software, and services with IPv6 supported/enabled. The work on addressing and routing has a strong relation to this area of interest.

Examples of our IPv6 *evangineering* work in 2010 are our participation in

- an IPv6 security workshop organized by TNO and GNKS consult; and
- a expert-group that recommended IPv6 to be placed on a the so called “deploy or explain” list for standards that are mandatory for governmental use[4].

3 http://www.enisa.europa.eu/act/res/technologies/tech/routing/state-of-the-art-deployment-and-impact-on-network-resilience/at_download/fullReport

4 http://www.open-standaarden.nl/actueel/item/titel/college-standaardisatie-plaatst-ipv6-en-ipv4-gezamenlijk-op-pas-toe-of-leg-uit-lijst-met-open-stan/

- Area of Interest: Standards Development, Internet Governance and technical advisories.

NLnet Labs staff is actively involved in the Internet Standards Development through involvement in the IETF.

Kolkman was reappointed as chair of the Internet Architecture Board in March 2010. As the IAB chair he is ex-officio member of the IESG, the IAOC, and is an IETF Trustee. Furthermore, NLnet Labs staff has actively participated or tracked the work in the BEHAVE, DNSEXT, DNSOP, ENUM, SHIM6, IDR and GROW working groups, and the Routing Research Group both in email discussions and during meetings. NLnet Labs staff is also participating in the RIPE meetings.

During 2010, Akkerhuis contributed as a paid consultant to ICANN, first for 5, and as of July 1 for 1.5 days per month.

As part of this role he is a member of the ISO 3166 Maintsenance Agency, ISO's focal point for country codes.

This year additional effort (separate from the ICANN related effort) was invested in this subject. The Kingdom of the Netherlands went trough a Constitutional reform. The Dutch Antilles ceased to exist as a country. Three of the Islands became Dutch municipalities, while Cura ç ao and Sint Maarten became separate countries[5]. We informed the various parties involved how this would effect the ISO standards and how the changes in these standards are made. Since there were a lot of parties involved this was quite some effort. In the end the result is that the Kingdom of the Netherlands consist of 4 Countries: Aruba (AW), Curacao (CW), The Netherlands (NL) and Sint Maarten (SX) while the BES-Islands (Bonaire, Sint Eustatius & Saba) are a separate territory (BQ)[6].

Akkerhuis and Kolkman continued to participate in the DNSSEC deployment group that is 'hosted' by Shinkuro and funded by the US Department of Homeland Security. That group strives to coordinate global DNSSEC deployment efforts.

Both Kolkman and Akkerhuis are active in the area between technology and policy development: Both participated in the round table meetings organized by RIPE NCC. Akkerhuis en Kolkman are also arbitrators for the RIPE NCC Conflict Arbitration procedure.

Akkerhuis is a member of ICANN's security and stability advisory committee SSAC[7] and the Dutch IPv6 Task Force[8].

5 http://english.minbzk.nl/subjects/aruba-and-the/new-status-for-the
6 http://www.iso.org/iso/iso_3166-1_newsletter_vi-8_split_of_the_dutch_antilles_final-en.pdf
7 http://www.icann.org/committees/security/
8 http://www.ipv6-taskforce.nl

5 The future

5.1 DNS

NLnet Labs will continue with a focus on DNS related activities.

DNS is one of the technologies on which virtually all applications on the Internet depend for their availability and security. NLnet Labs develops software, tools, and expertise to improve the overall stability, security and resiliency of the DNS.

Our vision is to create a suite of software tools with comprehensive DNS management and control tools. Within that context we are currently focusing on OpenDNSSEC and additional “Swiss army knife” tools that allow for troubleshooting and early warning.

In 2011 we start developing NSD4 that is set out to support environments that have to support many zones in a dynamic fashion (see sidebar).

We continue to commit to provide community support for NSD and Unbound, with a commitment to announce termination of such support at least 2 years in advance. This commitment provides users of our software business continuity, and thus contributing to the acceptance and dissemination of the technology. We are also committed to provide 3rd line support on OpenDNSSEC. A Swedish not-for-profit is established in 2011. It will provide 1st and 2nd line support, consultancy, promotion, and other OpenDNSSEC related activities.

5.2 And more

NLnet Labs' expertise on Internet System technology and architecture, focuses on the technologies in the 'waist of the hourglass': DNS, IP, and Routing. Technologies which benefit the users of the Internet at large, that provide security, stability, scalability, and reliance, and technologies that are crucial for further growth and maintaining openness of the Internet.

The IP protocol suite, in particular the openness of its addressing and routing technology, is key to the successful evolution of the Internet. There are, however, several challenges in the near future to allow the network to scale for the next billions of users and their devices to be connected. Because scaling issues are a threat to the open nature of the Internet. NLnet

Beyond NSD3

The NSD3 implementation is working well, NSD enjoys good performance due to its lack of features, and provides a stable implementation. It has been deployed on Root servers, a number of TLDs and also for other zones on the internet today. NSD does not use locks and threads, instead it uses processes and virtual memory. NSD makes memory-for-speed tradeoffs. NSD aims to provide an alternative DNS implementation for code diversity and is often deployed alongside others.

High Level Requirements

NSD3 lacks support for environments that have requirements for dynamic provisioning and/or serve zones that are dynamic in nature.

Rapid configuration changes

For NSD3 a change in configuration necessitates recompilation of the pre-compiled database (zonec) and a restart of the daemon. New zones also cannot be configured without a restart. Old zones cannot be removed without a restart either.

NSD4 needs the ability to add and remove zones without the restart, or recompilation of the database. In fact zones need to be added and removed without any service interruption.

Support for a high number of Zones

NSD3 works operates well when a low number of zones is configured. It has proven to be highly efficient for small zones like the root, and larger zones like the .NL TLD zone. However, it does not scale well to many zones (1000s or hundred thousands); it stops responding in a timely manner (to start, stop commands) when many zones are configured.

NSD4 will be efficient over a larger span of operational circumstances: from a few large zones to many small zones.

NSD4 remains to be optimized for the task of high performance DNSSEC aware name serving. It is typically not used for provisioning. Therefore support for dynamic updates is an explicit non-requirement.

Efficient incoming AXFR and IXFR supports the dynamic environments that NSD4 is targeted for – environments in which NSD4 is typically used as a secondary nameserver. Support for outgoing IXFR will only be provided if the implementation thereof does not add performance or complexity.

Performance, CPU, and memory

NSD4 performance should be (roughly) the same or better than NSD3. If during implementation of performance increasing measures trade-offs need to be made between optimization in memory usage or CPU usage (pre-compilation vs real-time compilation of packets) then the assumptions will be made that 32GB memory is available for entities that maintain 1 or more zones that collectively contain between 1 and 10 Million records.

Labs looks at scaling issues in the architecture. Both by investigating the necessity to create solutions and in investigating practical and deployable approaches to architectures that can solve mobility, scaling, and multihoming issues. As an independent expertise center on Internet architecture and technology with considerable experience in Internet Governance issues, NLnet Labs has acquired recognition in the field with a proven track record, and the corresponding responsibilities such as the involvement in several workshops about Internet Government issues, organized by the ministry of Economic affairs, Kolkman's role as IAB chair, and Akkerhuis' involvement in ICANN.

5.3 Long Term Outlook

NLnet Labs strives to be a technical expertise center that promotes the core values of an open, innovative, and collaborative set of networks: *the Internet*.

To that end NLnet Labs will continue to find pragmatic approaches to bridge between theory and practical deployment of Internet protocols. The specialism and expertise of the team determine which avenues are pursued. Exploration of new emerging areas relevant to the future of the Internet that fuel potential collaborations with other parties are inherent to the role NLnet Labs plays in the field. One of the main selection criteria for projects is whether our contribution makes a difference, whether our participation serves public interest and relates to an open and innovative Internet environment available to all.

6 NLnet Labs organization and finance

6.1 Board

NLnet Labs Board in 2010		
name	**title**	**end of term**
Frances Brazier	secretary	December 28, 2011
Simon Hania	member	Resigned May 2010
Frans Kollee	prospective member	Since November 23, 2010
Ted Lindgreen	member	January 31, 2012
Wytze van der Raay	treasurer	December 28, 2013
Leo Willems	chair	February 1, 2013

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its Board consists of three to five members with staggered terms. In 2010 Simon Hania resigned from the board and Frans Kollee joined. The board's composition and most recent rotation schedule is shown in the table.

Five board meetings took place in the year 2010: 9 February, 18 May, 14 September, 12 October, and 23 November All meetings took place in Amsterdam. Olaf Kolkman participated in the board meetings in his role of Director of NLnet Labs.

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€ 270 for 2010). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

6.2 Staff

NLnet Labs employed six people in 2010: Jaap Akkerhuis, Olaf Kolkman (director), Wouter Wijngaards, Benno Overeinder, Matthijs Mekking, and Yuri Schaeffer. Shaza Hanif joined labs for a 6 month internship as part of the VU computer science master course. Jop Schinkel performed a 1 day high-school *snuffel-stage*. Recruitment effort was started during the year to fill the new support engineer position, the selected candidate starts in January 2011.

The director of Stichting NLnet Labs is responsible for the daily management of all activities of the Open Source network software development laboratory, including development of strategies and plans for new activities.

Director and Board Member Additional Functions in 2010	
name	additional functions
Frances Brazier	Professor Engineering Systems Foundations at the Technische Universiteit Delft (TU Delft) Vice-chair of the board of Landelijk Netwerk Vrouwelijke Hoog-leraren (LNVH)
Simon Hania	Senior Vice President Publishing TomTom
Frans Kollee	Senior security consultant Madison Gurkha
Ted Lindgreen	none
Wytze van der Raay	Treasurer Stichting SANE Team leader CAcert critical system administrators
Leo Willems	Director TUNIX Internet Security & Training. Member of the board of Stichting IT Projecten (StitPro).
Olaf Kolkman	Chair Internet Architecture Board Ex-officio member of the Internet Engineering Steering Group, the IETF Administrative Oversight Committee, and an IETF Trustee Arbiter for the RIPE NCC Conflict Arbitration Procedure

6.3 Finances

Stichting NLnet Labs primarily finances its projects and activities from grants obtained from its parent organization Stichting NLnet. The long term financial commitment of NLnet towards NLnet labs has been codified since 2007 in a subsidy contract with a five year notice period. This allows NLnet Labs to commit to long term efforts and support.

A second means of income are subsidies and donations by other parties. NLnet Labs has developed a sponsor agreement. For 2010 we would like to acknowledge AFNIC and Comcast for their generous support.

In addition, income may be obtained by providing Open Source Internet based consultancy and/or programming services to third parties. A consultancy contract with ENISA, DNSSEC training, and a number of NSD support contracts were sources of additional income in 2010 in the latter category.

Acknowledgements

In 2010 the NLnet Labs foundation received subsidy and donations from

nlnet FOUNDATION comcast .fr AFNIC

See http://www.nlnetlabs.nl/labs/contributors/ for more information

6.3.1 Fiscal Status

On 20 September 2007, NLnet Labs has been recognized as a 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.

6.3.2 Income in 2010

At the end of 2009, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2010, with a total of € 611.580. Based on this budget and the expected consultancy income, a grant was requested from Stichting NLnet for € 502,000 during 2010. Stichting NLnet allocated these funds for 2010, to be received by NLnet Labs on a quarterly basis, € 125,500 per quarter. By the end of 2010 it became obvious that the requested budget would be more than needed to cover 2010's costs this was mainly due to having budgeted for a support engineer which we only managed to acquire and contracted at the end of

Income 2010

	2009 actual	2010 actual	2010 budget
NLnet Subsidy	390,000	402,000	502,000
Other Donations	10,000	31,017	15,000
Consultancy Income	98,000	86,650	48,000
NSD & Unbound Support	43,750	51,538	44,500
Interest Income	3,900	1,920	1,200
Total	545,650	573,125	610,700

2010 and who joined in 2011, and not budgeted consultancy and subsidy income totaling. At the end of the year, € 100,000 subsidy could thus be returned to NLnet. The net result is that during 2010, Stichting NLnet Labs received a total of € 402,000 from Stichting NLnet and a total of € 31,017 in donations (from Comcast and AFNIC).

The consultancy contract with ICANN from April 2005 was continued in 2010, but its scope was narrowed to 1.5 days per month as of July 2010.. Besides, NLnet Labs offers support contracts for NSD and Unbound. The total income from consultancy and NSD support in 2010 came to € 138,188.

The only other significant source of income during 2010 was interest derived from a savings account used to deposit funds temporarily. This amounted to € 1,920.

2010 Expenditure

	2009 actual	2010 actual	2010 budget
Staff	432,214	450,104	474,000
Housing	39,001	39,598	39,900
Travel	34,026	43,453	42,000
Depreciation	3,459	3,515	6,000
Other costs	36,085	35,488	46,680
Total	544,785	572,158	611,580

6.3.3 *Expenditure in 2010*

The major expenditure categories of NLnet Labs in 2010 are staff, travel and housing.

Over 2010 NLnet Labs had a positive result of € 967.

As a result, the financial reserve at the start of 2010 is € 67,190.

The NLnet Labs books have been audited by Koningsbos Accountants BV from Amsterdam on May 12, 2011.

6.3.4 *Budget for 2011*

The 2011 budget has been drawn up in October 2010. The main increase in expenditure is caused by having contracted 1 additional support engineer as of 1 January 2011. This support engineer will allow us to cope with the increased support pressure caused by the popularity of our products.

NLnet Labs expects to receive about € 16.500 from consulting activities, € 15,000 though donations, and € 57.000 from support contracts. To cover the projected deficit for 2010 a request for four quarterly grants of € 135.500, thus for a total of € 542.000 in 2010, has been submitted to Stichting NLnet, and has been granted on 9 December 2010.

2011 Budget

	2010 actual	2011 budget
Staff	450,104	515,400
Housing	39,598	43,300
Travel	43,453	42,000
Depreciation	3,515	4,800
Other costs	35,488	45,240
Total	572,158	650,740

6.3.5 *Financial Outlook*

In December 2010, Stichting NLnet has formally announced that it will terminate this subsidy contract by December 31, 2015, due to an expected lack of funds by that time. Director and board are starting an intensive effort in 2011 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.

7 Publications, Presentations, and Report

7.1 Publications

Hanif, S., “Impact of Toplogy on BGP Convergence”, MSc. Report, Department of Computer Science, VU University Amsterdam, August 2010.

Overeinder, B.J., and Botterman, M., “Secure Routing: State-of-the-Art Deployment and Impact on Network Resilience”[9], ENISA report, September 2010.

Schaeffer, Y,”K-root TCP load measurements”[10], NLnet Labs document 2010-001, February 2010.

Schaeffer, Y, “NSEC3 Hash Performance”[11],NLnet Labs document 2010-002, March 2010.

Schaeffer, Y, “SIDN Server Measurements”[12], NLnet Labs document 2010-003, July 2010.

7.2 Presentations and meetings participation

14 January, ISOC.NL new years event, Kolkman moderated the chair-debate.

28-29 January, Mekking, OpenDNSSEC all-hands meeting, Amsterdam, NL.

1-3 February, Kolkman, “2nd Annual Global Symposium on DNS Security, Stability, and Resliency, Kyoto, JP.

4 February, Kolkman, DNSSEC lecture at the Tokyo University, Tokyo, JP.

5 February, Kolkman, lecture at JPNIC, Tokyo, JP.

2-7 February, Schaeffer and Wijngaards, Unbound Training, Iceland.

15-16 February, Overeinder, LINX Community Meeting, London, UK. Presentation on ENISA survey on routing security state-of-the-art and deployment.

18 March, Overeinder, ICT Delta, Rotterdam, NL. DNSSEC for a wide (non-technical) audience.

21-26 March, Akkerhuis, Kolkman, Mekking & Overeinder, IETF 77, Anaheim, CA, US. Mekking presented the NSEC3 Hash Performance research to the DNSOP working group[13], Kolkman worked on RFC4641bis[14] and Trust History[15] in the DNSOP working group. Mekking participated in the IETF Code Sprint.

27-28 April, Kolkman, IAOC Retreat, Geneva, CH.

1-2 May, OARC Meeting, Prague, CZ.

3-7 May, Akkerhuis, Kolkman, Mekking & Overeinder, RIPE 60 meeting, Prague, CZ. Overeinder presented ENISA routing security study[16].

25-26 May, Kolkman, IESG Retreat, New York, NY, US.

31 May-3 June, Kolkman, Terena Networking Conference 2010, Vilnius,LT. Kolkman presented on NLnet Labs activities[17] and gave an update on the IETF[18].

8-9 June, Kolkman, IAB Retreat, Cambridge, MA, US.

22-23 June, Mekking, OpenDNSSEC Code Sprint, Oxford, UK.

22-24 June, Akkerhuis & Kolkman, ICANN 38, Brussels, BE.

9 http://www.enisa.europa.eu/act/res/technologies/tech/routing/state-of-the-art-deployment-and-impact-on-network-resilience/at_download/fullReport
10 http://www.nlnetlabs.nl/downloads/publications/k-root_tcp_measurements.pdf
11 http://www.nlnetlabs.nl/downloads/publications/nsec3_hash_performance.pdf
12 http://www.nlnetlabs.nl/downloads/publications/sidn_measurements.pdf
13 http://www.nlnetlabs.nl/downloads/presentations/nsec3hp_dnsop_ietf77.pdf
14 http://www.ietf.org/proceedings/77/slides/dnsop-3.pdf
15 http://www.ietf.org/proceedings/77/slides/dnsop-2.pdf
16 http://www.nlnetlabs.nl/downloads/presentations/RIPE_Routing_Security_Survey.pdf
17 http://tnc2010.terena.org/core/getfile.php?file_id=297
18 http://tnc2010.terena.org/core/getfile.php?file_id=306

30 June-1 July, Kolkman, Global Cyber Security Center DNSSEC Awareness and Planning Workshop, Rome, IT.

1 July, ENISA's and RAND Europe's Workshop on Incentives and Challenges for Information Sharing, Brussels, BE.

25-30 July, Akkerhuis, Kolkman, Mekking, Overeinder, Wijngaards, IETF 78, Maastricht, NL. Overeinder presented at the IEPG on main results of ENISA report[19]. Kolkman worked on RFC 4641bis[20] and Mekking presented the auto-cpsync draft[21]. Mekking participated in the IETF Code Sprint.

2 August, Kolkman, IETF-ITU-T leadership meeting, Geneva, CH.

4 August, Mekking, Devnology, Zoetermeer, NL. Presented "DNS at NLnet Labs"[22]

28-August, Akkerhuis, Expert Workshop at TNO, "Indicatoren voor betrouwbaarheid en veiligheid van ICT", Delft, NL.

9 September, Akkerhuis & Kolkman, RIPE Arbiters meeting, Amsterdam, NL.

10 September, Akkerhuis, RIPE WG Chair meeting, Schiphol, NL.

6-8 October, Akkerrhuis, 43rd CENTR Global Assembly, Brussels, BE.

19-23 October, Akkerhuis, SSAC retreat, Arlington, VA, US.

15-19 November, Overeinder, RIPE 61, Rome, IT. Co-organized RPKI workshop.

8-9 December, Kolkman, IAB, ISOC, W3C Privacy Workshop, Cambridge, MA, US

14 December, Kolkman, Meeting DG INFSO and IETF-leadership, Brussels, BE.

19 http://www.nlnetlabs.nl/downloads/presentations/Routing_Security_IEPG_IETF_78.pdf
20 http://www.ietf.org/proceedings/78/slides/dnsop-1.pdf
21 http://www.ietf.org/proceedings/78/slides/dnsop-2.pdf
22 http://www.nlnetlabs.nl/downloads/presentations/devnology-20100804.pdf

NLnet Labs
Science Park 400, 1098 XH Amsterdam
e-mail: labs@nlnetlabs.nl, web: http://www.nlnetlabs.nl/