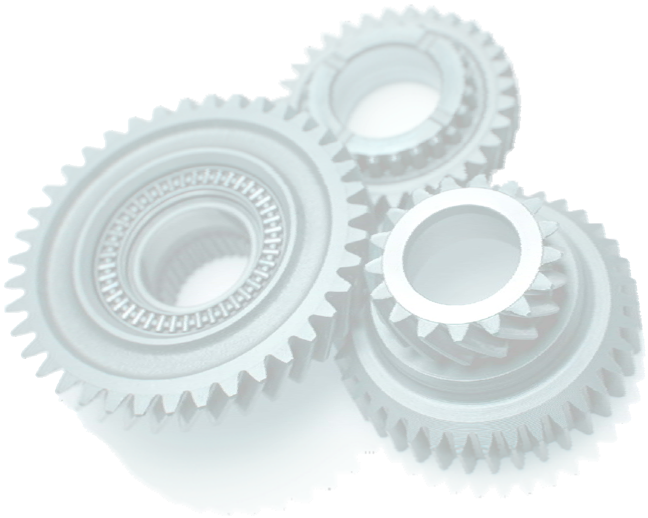


ISC News

October 1, 2009

Volume 1, Issue 1

The Future: BIND 10

By Shane Kerr, BIND 10 Programme Manager

BIND 10 is, briefly, a re-design and re-write of BIND 9. BIND 9 is itself a re-design and re-write of BIND 8. BIND 9 is by far the most widely used DNS server on the Internet (one estimate is something like 80% of DNS servers [1]).

> *“We’d like as large a group of folks to join the fun as we can get”*

The ISC development model has been relatively closed to date (think "Cathedral"). This is not necessarily bad, but I want the BIND 10 development to be open, including exposing the details of various discussions and decisions made within the project. My hope is that publishing how and why we make the design choices we make will mean that the project will have usefulness beyond the software itself.

The BIND 10 project officially kicked off on 2009-04-01. In fact, ISC employees had been spending some of their time trying to define what the project is and how it was going to look for several years before that. But that work was unfunded and largely unfocused - other day to day business took precedence. One of those people was João Damas, who was able to convince a set of 10 initial organizations to donate substantial sums of money to ISC to create the software. You can see the list of current sponsors on the BIND 10 Sponsors page. So now we have sponsors, and just as important, we have an agreed-upon deliverable for the first year.

The year one deliverable is an authoritative-only DNS server, plus all of the necessary infrastructure that will be used for future development. This is probably the simplest form of DNS server: we need to be able to receive and process DNS messages, and reply with an answer from some sort of database (BIND 9 uses zone files to load an in-memory data structure, but in fact this database can be anything).

There are several ways to follow and get involved in the BIND 10 effort. We've got a Trac site set up , a public developers mailing list, a ton of design discussions, a rough project plan... and now the blog and newsletter.

As far as the actual project, I invite everyone to subscribe to the bind10-dev list, and look at the development site for details as they arrive. We'd like as wide a group of interested people joining in the fun as we can get.

One of the goals of BIND 10 is a pleasant administrator experience, but we'll need your feedback to know if we're achieving that. This fall we will be reaching out to the community for feedback on user interface design. We welcome and value your input.

Resources:

Trac:
bind10.isc.org

Sponsors:
www.isc.org/bind10/sponsors

dev list:
lists.isc.org/mailman/listinfo/bind10-dev

Bind10-announce list: *lists.isc.org/mailman/listinfo/bind10-announce*

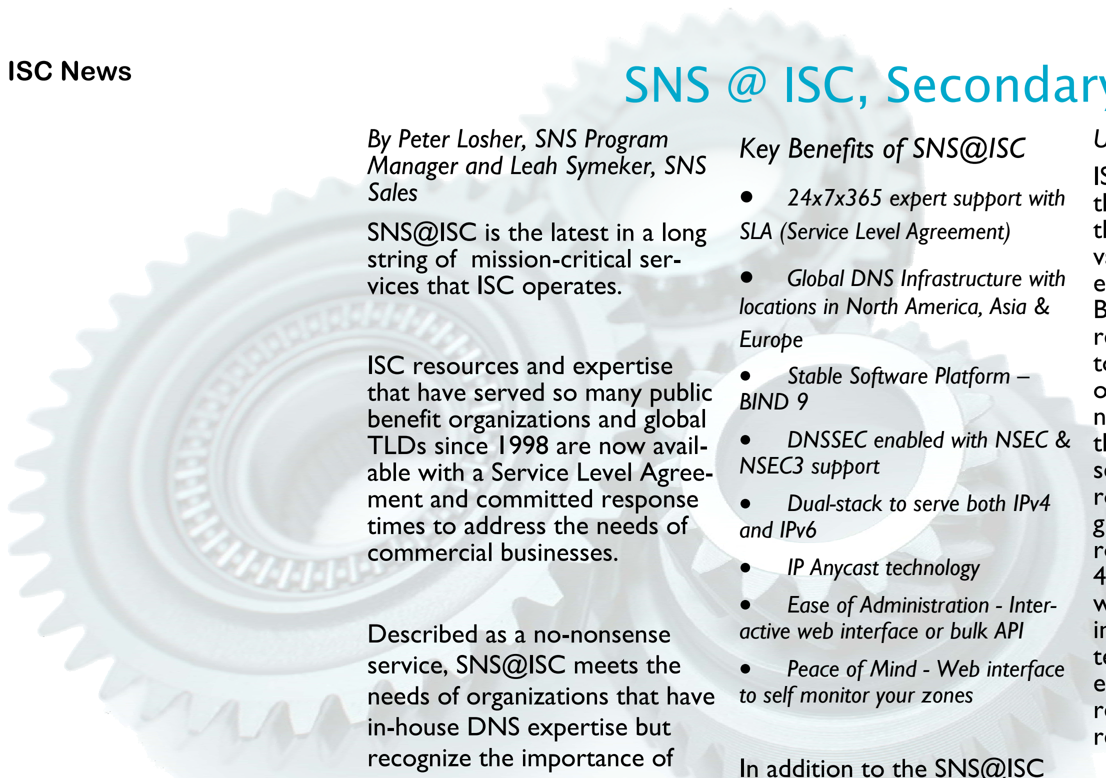
Support us:

www.isc.org/donate/bind-10

References:

[1]http://ftp.isc.org/www/survey/reorts/current/report.fpdns

Inside this issue:



SNS @ ISC, Secondary DNS Hosting

By Peter Losher, SNS Program Manager and Leah Symeker, SNS Sales

SNS@ISC is the latest in a long string of mission-critical services that ISC operates.

ISC resources and expertise that have served so many public benefit organizations and global TLDs since 1998 are now available with a Service Level Agreement and committed response times to address the needs of commercial businesses.

Described as a no-nonsense service, SNS@ISC meets the needs of organizations that have in-house DNS expertise but recognize the importance of DNS uptime and additional network diversity. SNS@ISC is straightforward, highly reliable and provides our customers full control of their DNS data. Our clients manage their primary nameservers and SNS@ISC provides DNS redundancy ensuring 100% delivery of their zone data to the internet using ISC's global DNS infrastructure.

Key Benefits of SNS@ISC

- *24x7x365 expert support with SLA (Service Level Agreement)*
- *Global DNS Infrastructure with locations in North America, Asia & Europe*
- *Stable Software Platform – BIND 9*
- *DNSSEC enabled with NSEC & NSEC3 support*
- *Dual-stack to serve both IPv4 and IPv6*
- *IP Anycast technology*
- *Ease of Administration - Interactive web interface or bulk API*
- *Peace of Mind - Web interface to self monitor your zones*

In addition to the SNS@ISC commercial offering, ISC continues to offer no charge DNS hosting to any qualifying organization, that is non profits, educational institutions, and ccTLDs on a best-effort basis. For more information on SNS@ISC and how we can address your needs please send email to SNS@ISC.org.

Uniquely Qualified

ISC has been a driving force in the DNS market place since the beginning resulting in unrivaled expertise and experience. ISC puts our software, BIND, to one of the toughest real-world tests as the operator of F.root -servers.net, one of the busiest of the 13 root nameservers. ISC pioneered the globally distributed root server model by installing F-root nameservers around the globe. The total number of F-root installations is now over 45 locations worldwide. ISC with F-root have led the way in pairing DNS and Anycast technology in a production environment to enable faster response times and increased reliability.

Hosted@ISC has been providing web hosting & mirroring services to widely-used open source projects such as the Linux Kernel.org, FreeBSD & Mozilla for over 10 years.

Please visit the ISC website at https://www.isc.org/solutions/sns for more information.

"ISC puts our software to one of the toughest real-world tests as the operator of f.root-servers.net, one of the busiest of the 13 root nameservers. "

New End of Life and Support Policy

By Sue Graves, Client Services Manager

ISC's revised Software Support Policy, effective August 28th, 2009

We have listened to input from our OEM and Enterprise customers, who have difficulties with the change management time frames involved in our current Support and End of Life Policy. ISC is pleased to announce the addition of an Extended Support Version release to our current release offerings and support policy.

We will continue our existing policy to support the current release plus one previous Feature release.

Six months after a new feature release (9.x), the feature release two versions back will go End-Of-Life (EOL). Currently, we intend to publish major feature versions nine to twelve months apart.

For our users who have longer upgrade constraints, we will establish a new option for both BIND and DHCP called Extended Support Version (ESV) which will be supported for three years. Only critical bug fixes and security fixes will be added to the ESV releases. Eighteen months into the life of an ESV release we will select a new three year ESV candidate, so that there is a continuous flow of ESV releases.

Upcoming ESV releases:

- BIND:BIND 9,4-ESV, established mid-cycle, to be supported for six months to Feb, 2010.
- BIND 9.6-ESV (to be supported for the full 3 years)
- DHCP 3.1-ESV (at one year into its release cycle now, it will EOL September 2011)
- DHCP 4.2-ESV will be the second DHCP ESV release, available in early 2010.

This policy is subject to change. ISC may elect to add minor features into point releases going forward. Policies do not apply to pre-release code. Developmental releases may follow different schedules.

BIND 9.7: DNSSEC for Humans

By Jeremy Reed, ISC Technical Writer

The challenges of keeping up with DNS security are many. DNSSEC extends standard DNS to prove the data is not modified and came from the official source. ISC BIND supports the full DNSSEC standard. The new release of BIND 9 includes substantial improvements to ease of use for DNSSEC. *BIND 9.7 will be available in December 2009, with a beta available in early October.*

The following are some of the planned features for BIND 9.7.0:

- *Automated trust anchor maintenance for DNSSEC (RFC 5011)*

RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors, documents a method for automated, authenticated, and authorized updating of DNSSEC "trust anchors" especially for the use of multiple islands of trust.

The new managed-keys statement provides named with trusted keys which are automatically kept up to date using RFC 5011. It differs from the trusted-keys statement with an additional field (second field) containing initial-key keyword which means only use this key the first time. named stores keys in a managed keys database.

- *Simplified configuration of DNSSEC Lookaside Validation (DLV)*

A new configuration setting auto was added for the dnssec-lookaside option. This enables DLV by using the dlv.isc.org repository and provides a built-in trusted key for it. The hard-coded trusted key can be overridden by placing it in a $sysconfdir/bind.keys file.

- *Simplified configuration of Dynamic DNS*

The update-policy zone option has been extended to add a local setting to enable Dynamic DNS for a zone. named will generate a TSIG session key known as local-ddns at startup which will be used for these updates. The session key file defaults to /var/run/named/session.key or can be defined using the session-keyfile option.

The nsupdate tool now has a -l switch to tell it to sign updates using the generated session key and to send the update requests to the localhost. The new ddns-confgen tool may be manually used to create a local authentication key and generate an example configuration for named.conf and the nsupdate syntax.

With these new dynamic DNS features, it is also now easier to configure automatic zone re-signing for DNSSEC.

- *Share view caches with new option "attach-cache"*

The new attach-cache option allows multiple views to share a single cache. When configured, at named start up, it will attempt to reuse an existing cache if possible for a view to save memory and improve lookup efficiency. (It does not use previously stored cache from disk.) This feature is based on contributed code from Google.

DNS rebinding attack prevention named can now filter responses from remote DNS servers based on addresses or CNAME/DNAME targets in the answer section. The new deny-answer-addresses option can reject address records if matches an ACL list. The new deny-answer-aliases option can reject CNAME aliases or DNAME names if they match a name list. If it matches, the answer is not cached and a SERVFAIL response is returned. This can be used to filter outside responses from returning an answer that is within your own network. This feature is based on contributed code from Google.

For information about DNS rebinding attacks, see [1]http://portal.acm.org/citation.cfm?id=1315245.1315298 and

[2]http://en.wikipedia.org/wiki/DNS_rebinding.

- *Fully automatic signing of zones*

It is also planned that BIND 9.7.0 will named will be able to import keys from a key repository and start signing. The private key file format has been extended for setting key timing metadata. And new and extended DNSSEC command-line utilities provide simpler DNSSEC management.

- *Improved and extended libdns library*

The BIND 9 DNS libraries are available for use with third-party (non-BIND) applications. BIND 9.7.0 introduces new features including:

- DNS client API with support for DNSSEC and dynamic updates
- New "IRS" (Information Retrieval System) for parsing DNS configuration files.
- DNSSEC-aware getaddrinfo() and getnameinfo()
- Event task framework (experimental)

Additionally, PKCS#11 interface which was introduced in BIND 9.6 is improved and refined in 9.7. Improved HSM support will continue in future releases of BIND.

BIND 9.7 Beta Program:

ISC seeks participants in our open developmental release program for BIND 9.7. Interested parties please:

- *Join the beta discussion group at: lists.isc.org/mailman/listinfo/bind-beta-response*
- *Download BIND 9.7 alpha and beta releases at: www.isc.org/download/software/development*

Active participants will not just earn our sincere appreciation, but also a

BIND 9.7 t-shirt!

Coming Fall 2009

BIND and DNSSEC

Training in Rome

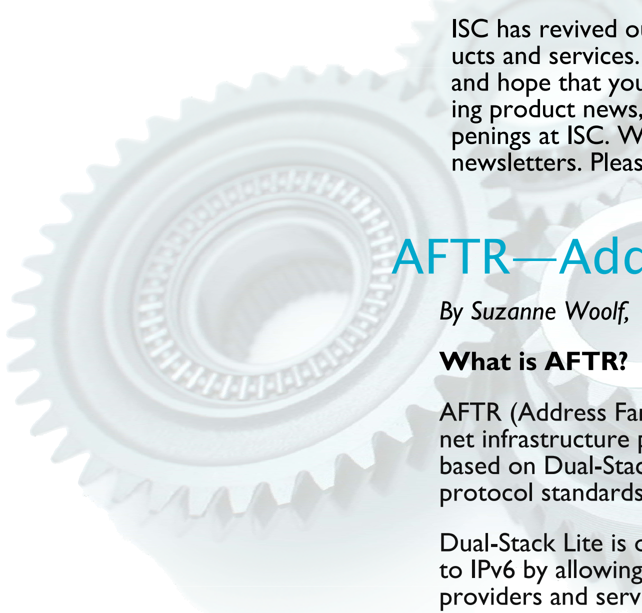
ISC and NaMeX are pleased to announce a partnership establishing NaMeX's Rome location as the primary European site for ISC's BIND and DHCP training courses. The first series of classes begins October 12th.

For more information please visit:

www.isc.org/services/training

Return of the Newsletter

ISC has revived our forum newsletter and updated the content to reflect all of our products and services. We will provide this newsletter to the community on a quarterly basis, and hope that you find it interesting and useful. The newsletter is meant to cover upcoming product news, any changes to our service offerings, events, or other newsworthy happenings at ISC. We are always interested in your feedback and suggested topics for future newsletters. Please send any feedback to info@isc.org.



AFTR—Address Family Translation Router

By Suzanne Woolf, Manager, Strategic Partnerships

What is AFTR?

AFTR (Address Family Translation Router) is the latest in ISC's family of open source Internet infrastructure products. It is an implementation of an IPv4/IPv6 transition protocol based on Dual-Stack Lite, which is under development by several large ISPs within the IETF protocol standards development process.

Dual-Stack Lite is one of a family of technologies intended to ease the transition from IPv4 to IPv6 by allowing legacy IPv4 end sites such as home PCs to interact with IPv4 content providers and services over an IPv6 carrier infrastructure. This allows ISPs to deploy IPv6 as the last available IPv4 addresses are allocated, without requiring expensive, complex technology changes immediately for end users or server operators.

Where Does AFTR Come From?

The initial version of AFTR consists of the code for a server that can give out either IPv4 or IPv6 addresses via DHCP, and tunnel via IPv6 to an arbitrary IPv4 endpoint elsewhere.

The initial development of ISC's AFTR was funded by Comcast over about 18 months in 2008 and 2009. However, AFTR was never intended for one carrier's use or benefit. It is an open source implementation meant to promote the development of open standards for IPv4/v6 transition technology. We're now inviting ISPs and enterprises-- anyone who needs to grow a network beyond the end of the unallocated IPv4 address space-- to join the AFTR community we're building and help make Internet growth happen beyond the end of the IPv4 address pool.

How Do I Learn More?

First, download the AFTR code, which can be found at https://www.isc.org/download. Version 1.0 is a basic implementation of the current proposed protocol, but both the code and the protocol are still under development. Try out the code, tell us how you use it, tell us how it could be more useful.

For more detailed information, read the presentation (www.arin.net/participate/meetings/reports/ARIN_XXIII/pdf/sunday/dealing_with_reality.pdf) Alain Durand made at an ARIN meeting this past Spring. Join the AFTR mailing lists, too, at the ISC Mailing List page (lists.isc.org/mailman/listinfo).

We're interested in your experiences with the code, bug reports, feature suggestions, and ideas for future development of both the code and the protocol.

Stay up to date with ISC executive musings, product design process, new releases, and more— learn and participate on the ISC Blog at ***blog.isc.org***

Upcoming ISC Releases:

October 2009:

- BIND 9.7 Beta
- BIND 9.4-ESV
- BIND 9.6-ESV
- DHCP 3.1-ESV
- DHCP 3.1.3

November2009 :

- BIND 9.6.2
- DHCP 4.0.2
- DHCP 4.1.1

December 2009:

- BIND 9.7
- DHCP 4.2

Internet Systems Consortium
950 Charter Street
Redwood City
California
94063
www.isc.org
info@isc.org

Internet Systems Consortium, Inc. (ISC) is proud to be the producer and distributor of commercial quality Open Source software for the Internet Community and to offer world-class online and professional services based on our software. Since 1996 ISC has led the industry with the most complete reference standard implementation of DNS (BIND) software using a Managed Open Source model. ISC also provides production-quality reference implementations for other core protocols such as DHCP, and distributes other open-source software. Managed Open Source means that users benefit from community ideas, while quality and compliance are the responsibility of professional software engineers. ISC also provides a number of Operational Programs and Services that benefit users of the Internet directly and indirectly. Since 1994, ISC has operated F-Root (one of the 13 root DNS servers) as a public service to the Internet.

ISC is a nonprofit 501(c)(3) public benefit corporation dedicated to supporting the Internet community with software essential to its infrastructure.