ISC SOFTWARE GUILD

BIND Forum Newsletter

BIND Forum Newsletter Launch

Volume 1, Issue 1

March 2004

Inside this issue:

Welcome to the first issue of the BIND Forum newsletter.

With this newsletter ISC aims to open a new communication channel with all BIND Forum members. We intend to publish the newsletter quarterly and use it to provide a reference for information on ISC activities, particularly those related to the BIND Forum, and developments in the world of DNS.

During the last few months a lot of events have taken place at ISC and in the world of DNS.

October of 2003 marked the launch of ISC's OARC for DNS, a new programme tasked with monitoring, reporting and analysis of the Internet's Domain Name System. [1]

As of January 2004, ISC has changed its named from Internet Software Consortium to Internet Systems Consortium. This change is far from being a cosmetic one and we encourage our readers to find out more about the details in a separate article on this issue.

In addition, the last few months have marked the successful worldwide deployment of the F root server through the use of a hierarchical anycast technique, bringing increase resilience to the Internet's DNS and the root server system in particular, as well as providing a closer server for Internet communities that previously were far away from any of the root servers. A future issue of this newsletter will have an article on the use of this technique for DNS services.

With regards to DNS protocol development, we are happy to see the IETF's dnsext working group working towards the final specifications of the DNSSEC protocol extension. In this issue's BIND column, you will find an article on ISC's position on DNSSEC support in future releases of BIND.

[1] http://oarc.isc.org

BIND Forum & ISC's Software Guild

With ISC's new structure comes a new framework for the BIND Forum – the ISC Software Guild.

ISC Software Guild, will house Fora for ISC's main software development projects.

Currently the BIND Forum is the only of these fora, but it a DHCP Forum will join it later in the year and others will be created as the need arises.

ISC CHANGES NAME

As of January 2004, Internet Systems Consortium has replaced Internet Software Consortium.

With this change, ISC updates its charter to better reflect its current activities, which in addition to development of reference implementations of core Internet protocols, extend to operational activities such as the F DNS root server, operation of secondary name service for a significant number of top-level domains, hosting facilities for open source projects and the recently launched DNS.

Together with the updated charter, the new ISC has a new legal status as a corporation in the State of Delaware, USA and has US Federal 501(c)(3) non-profit status.

Together with all these changes, comes a new web site, with a more straightforward layout for easier navigation. ISC is working towards extending this web site to be a true portal enabling members of ISC programmes to have a unique entry point for all services.

BIND

BIND 9

For some time now, ISC has been hard at work preparing the new feature release of BIND 9. All this work will come together in March 2004 when ISC releases BIND 9.3

BIND 9.3 will incorporate a huge amount of new features to support new protocol extensions and to offer better support to BIND administrators.

One of the most significant additions is the inclusion of code to implement the current draft specifications for the DNSSEC protocol extensions. Even though the specifications have not been completely finalised at this stage, ISC believes them to be close enough to their final form that the release of code enabling users to better understand the new functionality is the right thing to do.

BIND 9.3 will ship with DNSSEC support turned off by default in the configuration file given the unfinished state of the protocol and the experimental nature of the code at this point. Only the use of a new configuration option will enable this new functionality ensuring that current users will not encounter problems when upgrading their current systems. With this course of action, ISC supports protocol development at the IETF, enabling field-testing for the new technology.

There are many more additions coming to BIND 9.3. These provide better support and control for system and zone administrators. Here is a list of the most important new features:

- improved support for IXFR.
    - Incremental transfer data can be generated from difference in zone file versions, without the need for journal file creation.
    - Control over the journal file size.

- finer control over RRset ordering
- improved control over responses when using IPv6 transport and records
    - preferred glue allows for the selection of what glue records to include when not all of them fit in a DNS response packet.
    - transfer source address, for both IPv4 and IPv6
    - tag dual stack servers
- better control over cache-size. Now is effective at limiting the maximum size of BIND 9 cache when running as a recursive server.
- support for servers with multiple addresses.
- new server identification support (server.id)
- support for view selection based on TSIG key used.
- more powerful control of IP transport
    - select UDP ports (IPv6 and IPv4)
    - control of TCP listen queue length
- implementation of memory statistics
- implementation of configurable entry points for dnssec validation.

BIND 8

The current release of BIND 8 is 8.4.4, a maintenance release of BIND 8 fixing some bugs that have been detected since the release of BIND 8.4.

BIND 8.4.x is the last family of BIND 8 software and only maintenance work is being done. All new features are incorporated into BIND 9.

The Future

During 2004 ISC expects to release an additional feature release for BIND9, BIND 9.4. The current expected release schedule is late Q3.

Subject to discussion with BIND Forum members, the features that are expected to be included in BIND 9.4 are:

- production release of DNSSEC support
- support for GSS-TSIG transactions
- improved statistics
- improved performance, including, among others:
    - to shorten zone re-loading time.
    - new cache for authoritative servers that stores responses computed to previous queries, reducing the need for internal tree lookups.

DNS & BIND VISION STATEMENT

OVERVIEW

DNS -- the Domain Name System -- is the world's first and only distributed, coherent, autonomous, reliable database. Globally maintained by parties only distantly related, yet globally accessible by parties completely unrelated. Robust and reliable during all acts of god or of men, whether accidental or malicious. Its rules and specification are open and royalty free, subject only to the community of interest who controls its evolution.

Nearly all Internet applications, including e-mail, peer to peer file sharing, and the World Wide Web, depend on DNS for connection opportunities and direction. Almost every TCP/IP traffic flow on every Internet backbone begins with one or more DNS transactions. Every new Internet application now being contemplated includes some kind of DNS component, whether that's VoIP and ENUM, RFIDspace, resource discovery, or others.

At ISC, we believe that DNS is the key to the Internet's continued growth and relevance, just as we believe that the Internet is the key to global peace and prosperity in the 21st century -- and perhaps beyond. We produce BIND in order to ensure that DNS remains an open, robust, and extensible framework upon which new generations of products, services, and communities can base their work.

HISTORY

BIND (through 4.8.3) was first produced at U C Berkeley in 1983 and then carried forward by Digital Equipment Corporation (4.9 through 4.9.1), Vixie Enterprises (4.9.2), Internet Software Consortium (4.9.3 through 8.4.3 and 9.2.3), and finally by Internet Systems Consortium (8.4.4 onward, and 9.3.0 onward). BIND has always been made available under a simple license which allows unlimited redistribution in any form without fee, to encourage embedding of the whole system or any of its components.

Today BIND is the predominant DNS implementation on the visible Internet, running 80% of the nameservers discovered by ISC's Domain Survey (see <http://www.isc.org/ops/ds/reports/2004-01/dist-servsoft.php> for details.) While ISC welcomes other implementers, whether proprietary or open source, we feel quite strongly that the Internet's growth to date and prospects for the future rely on BIND's ability to keep the DNS playing field "level."

TRENDS

The DNS protocol has matured considerably since the formation of the IETF DNSIND working group in 1996. DNS now supports incremental zone transfers, real time notification of zone changes, dynamic (in-band) zone updates, transaction security by digital signatures, domain tree aliasing, and a handful of new record types including service location pointers, static routing advertisements, and geographical location information. The protocol has been extended to relax several constraints and pave the way for more enhancements in the future.

BIND has kept pace with these changes, and has been the first implementation to support every new protocol feature added since 1983. Often, protocol changes are prototyped using BIND before being formally proposed as standards, owing to BIND's wide popularity and ease of modification. ISC has always welcomed feature contributions from the community, and acts as a governor and clearinghouse to ensure that the software neither lags nor leads the standards process.

In recent years, the unique nature of DNS has led to its use in unforeseen areas such as e-mail policy enforcement (so-called DNS black hole lists, the first of which was called the Vixie RBL and later the MAPS RBL.) Because data entered into any part of the DNS is efficiently and reliably available to the whole Internet, it has become a channel for information quite unlike the host names, IP addresses, and e-mail pointers carried two decades ago.

TXT records (free form text) have been used to carry UNIX configuration data (as in MIT Hesiod), Internet Exchange Point (IXP) peering contact information, and even descriptive text for hosts reachable through terminal servers. SRV records (service pointers) are used today for resource discovery in Apple Macintosh (and compatible) networks in many homes and campuses.

Increasingly, the data being entered into DNS comes not from human operators but from other automated systems, and is consumed indirectly, after aggregation with other DNS or non-DNS data, or consumed not by human users but by other automated systems.

At ISC, we think this is all good.

BIND NEEDS

The user community for DNS and BIND is both vocal and connected. Many have spoken, and ISC has paid attention to their compliments, complaints, questions, and requests. We know that the following requirements should be met urgently in order to support the current high-growth areas of the Internet technology community.

1. BETTER DOCUMENTATION.

BIND's documentation has historically been very thin, such that many requests for new commands, options, or library functions are actually documentation bug reports -- the feature being requested already exists but the only way to learn about it is to read the source code or ask a wizard. We need new documentation, for nameserver operators, domain administrators, application developers, and system integrators. Library documentation should be bonded to, and generated from the source code, so that it will stay "up to date" in the future.

2. BETTER DIAGNOSTICS.

BIND's diagnostics are written in American English, without benefit of message catalogues, with an inconsistent style, and using obscure terminology which is not very helpful to non-wizards. We need to address each of those problems, such that a running BIND server or utility will emit consistent, useful diagnostics under both normal and exceptional conditions. Message catalogues must be employed to make internationalization possible for our integrators. To the extent possible, we must ship multiple message catalogues to support the non-English-speaking user community.

3. BETTER PERFORMANCE.

BIND9 is slower than BIND8 on a uniprocessor, and much to ISC's continuing embarrassment, BIND9 is slower on a multiprocessor than on a uniprocessor of equal clock speed. We must continue to shorten codepaths, remove excess generality, optimize hot spots, and localize data references. We must redesign our task management to take positive advantage of multiprocessors and threading. We must add the capability of compiling zones offline and doing fast-reload using memory mapping. BIND9 must be made able to take complete advantage of whatever resources it is given.

4. BETTER INTEGRATION.

Much data that is destined to be published via DNS is held in or generated by other automated systems, for example SQL servers. Current technology calls for the data to be extracted or exported into DNS zone file format and then loaded into BIND by laborious textual parsing. We must make it possible for data to be published into DNS using BIND as a front-end protocol engine, and only extract data at the point of need. This will require very careful front-end caching, and must support in-band dynamic updates. In addition, BIND needs a plug-in architecture so that optional or third party features can be added without requiring source code.

5. BETTER COMMAND AND CONTROL

The BIND configuration file syntax is human readable but in today's community it is often generated by front end management systems such as web-based cluster managers. We should add an XML based configuration system which is more amenable to generation and modification by automated systems. Our existing configuration syntax should be a wrapper around this new XML based system. We should ship prototype GUI and CLI interfaces to make it possible to control BIND servers, or distributed clusters of BIND servers, without any visible "configuration file" as such.

6. BETTER LIBRARIES.

While users of scripting languages such as Perl now have advanced libraries for marshalling and unmarshalling DNS data, and for participating in DNS transactions, and generating and consuming DNS data, those capabilities are not available to users of compiled languages such as C, C++, and Java. We should work with the technical community and with the POSIX committee to define an advanced DNS API for C, C++, and Java to enable DNS-aware applications to be written in those languages without exposing any on-the-wire details to those application programmers.

A DHCP server or client should be able to send a secure dynamic update and learn the success/failure result of same without knowing field size or byte order. This should enable a whole new kind of application to use DNS as a channel for its application-specific data, or to generate and consume data used by other, preexisting DNS aware applications. Messages, records, transactions, and other DNS artifacts should be available as opaque objects and should be manipulable without knowing wire formats or reading RFCs. Apple Rendezvous, MIT Kerberos, MIT Hesiod, and every SMTP implementation ought to be able to manipulate their DNS-based data without knowing details of the DNS protocol.

7. BETTER QA/TESTING.

Visible commands, options, or APIs must be backward compatible, and exceptions must always be intentional and made in cooperation with the vendor/integrator and end-user communities. Compatible changes, when introduced, must be clearly documented in release notes and in a version history document.

DNS NEEDS

Some feature developments in the DNS field have yet to be standardized but are nevertheless quite compelling to DNS's community of interest. Examples of these include:

1. MULTICAST DNS.

Apple, Microsoft, and others have described a need for local resource discovery, automatic configuration, and disconnected operation which could be well met by multicast DNS and SRV records (service location pointers). We acknowledge this need but are concerned that IETF's process and politics will continue to prevent progress, and deployment, from occurring. We proposed to implement every experimental proposal in this area in order to see them field tested as broadly as possible. When or if IETF decides on a standard in this area, BIND ought to be able to enable it immediately.

2. DNS SECURITY.

For 11 years now, IETF has attempted to add security to the DNS protocol. During much of that time, BIND was the only experimental platform on which various proposals could be test-piloted. There is some chance that the year 2004 will see a final form of this much-anticipated protocol feature set, and ISC is ready to release a BIND version conforming to whatever that final form happens to be. We also expect to tune BIND as necessary to fill gaps in this protocol extension for many years to come. Adding authenticity will allow DNS to carry many forms of data previously thought to be "too sensitive" for insecure DNS. ISC thinks that's all good.

3. ZONE FORMATS.

Some kinds of data carried by DNS in recent years have put some stress on system and network resources due to the expensive need to map external data formats into standard DNS records. For example, DNSBL zones usually consist of hundreds of thousands of A (address) records, whose owner names have several decimal ASCII labels, and are very sparse. Using standard zone transfer (AXFR and IXFR) is prohibitively resource intensive, and some non-standard DNS implementations have evolved to optimize for this case. A standard way of improving zone transfer and storage efficiency must be defined, and BIND must implement it in order to serve the community's needs in this area.

4. GSSAPI SECURITY.

At least one vendor has extended the TSIG (transaction security signature) model to include GSSAPI key management for scalability. This feature (GSS-TSIG) is a useful addition to DNS, and BIND should support it. Intellectual property problems may limit the interoperability of our implementation somewhat, but basic transaction security should be supported whenever GSSAPI (or Kerberos 5) services are available.

5. MULTIPLE MASTERS.

Some vendors have re-engineered the master/slave zone server relationship in DNS in order to provide what they call "multimaster DNS". While problems of interoperability and healing have marginalized this feature thus far, it remains clear that the community sees a need for other ways to manage an authority zone beyond the traditional master/slave model. ISC should explore alternatives in this area using BIND for prototyping, and we should ultimately propose IETF standards in this area.

The future of DNS is wide open, and ISC wants BIND to remain at the leading edge of protocol conformity, adaptability toward experimental features, and community visibility and accessibility.

RELATED EFFORTS

ISC changed its name to Internet Systems Consortium, Inc. in January 2004, and is now a non-profit 501(c)(3) corporation incorporated in Delaware. Our new name better reflects our long focus on total systems, including development of software, operations, and protocols. In addition to BIND, we also produce the community's leading DHCP implementation, and are the caretakers of other widely used software including INN and BSD CRON.

ISC operates "F" root, one of thirteen root name servers which publish the "root zone" needed to glue the Internet's domain name system together, and in the last 12 months we have grown "F" root from two cities to twenty -- mostly in response to widespread "denial of service" attacks to which "F" root has been almost uniquely immune. ISC also hosts dozens of other Open Source projects in our data center without fee, including the NetBSD project, the Linux Kernel Archives, and mirrors for Mozilla, OpenOffice, FreeBSD, and more.

We recently launched ISC OARC for DNS, our Operations Analysis and Research Center, intended as a platform for monitoring and characterizing the global DNS as a real time operational system. This year we will also launch DNS-MODA in partnership with WIDE (in Japan) and NETNOD (in Sweden). This "Manufacturers, Operators, and Developers Association" will manage a coherent multi-vendor effort to see that DNS protocol development within IETF never falters due to overextended volunteers, and that standards proposals are well tested early in life.

ACCOUNTABILITY

ISC's board is drawn from the international technical and business community, and as a public benefit nonprofit corporation we are beholden to the public interest. We cherish our relevance and wherever possible we eschew controversy and confrontation in favour of consensus, negotiation, and cooperation.

CONCLUSION

ISC holds these truths to be self evident: that the Internet is essential to the peace and prosperity of humankind; that DNS is essential to the growth of the Internet; that BIND is essential to the stability and openness of DNS; and that ISC, through BIND and "F" root and OARC/DNS and as a partner in DNS-MODA and in a hundred smaller ways, is the means to all of those ends.

We ask the members of the BIND Forum of the ISC Software Guild to share our vision for the future of open source DNS software.