DNS Unbound – A New Generation of DNS Servers

Nominum®, Inc.
2385 Bay Road
Redwood City, CA 94063
(650) 381-6000

> www.nominum.com

Introduction

Nominum is in the unique position of having authored both BIND[1] 9 and our own commercial Domain Name System (DNS) server products, Nominum® Foundation™ ANS and Nominum Foundation CNS. This paper discusses the development history and the merits of each solution. It also explains a bit of Nominum's background, and why we decided to provide alternative world-class DNS solutions that complement BIND. A more detailed company history is available at www.nominum.com/company.php.

The BIND 9 Project

By 1998, it was widely understood that the aging BIND 8 DNS server architecture was not holding up well to constant revision. In addition, the Internet Engineering Task Force (IETF) had been publishing many new DNS standards to address such issues as the increasing security threats against the DNS and the proliferation of Internet Protocol (IP) connected devices. Due to the accumulated effects of years of code submissions by over 100 individuals, it was clearly far easier to write a new version of BIND than to shoehorn new IETF-defined functionality into BIND 8 as patches.

The non-profit Internet Software Consortium (ISC) develops and maintains open source reference implementations of core Internet protocols such as DNS and DHCP (Dynamic Host Configuration Protocol). The ISC worked with many parties, including the U.S. Department of Defense, major Unix hardware vendors, and international research institutes, to define the goals of a project to develop a new BIND, specify its features, and acquire the funding to complete the development project. Unlike BIND 8,which was based on the original Berkeley version of BIND, BIND 9 would be all-new code developed using modern software engineering techniques. The ISC would distribute BIND 9, but first they needed an elite group of engineers to write the code.

In 1999, David Conrad and Paul Vixie founded Nominum and accepted responsibility for writing BIND 9 according to the funders' specifications. Conrad and Vixie recruited some of the most highly esteemed Internet visionaries to join the small company. These included Paul Mockapetris who, in 1983, invented the DNS and wrote the original DNS RFCs[2], and Ted Lemon, the primary developer of ISC-DHCP and co-author of *The DHCP Handbook*[3].

[1] "Berkeley Internet Name Domain" server

[2] Request for Comments – the IETF's name for its Internet Standards document series

[3] *The DHCP Handbook 2nd ed.,* Ralph Droms, PhD & Ted Lemon, October 2002, Sams Publishing, ISBN 0-672-32327-3

Nominum released BIND 9.0 to the ISC in September 2000. As of mid-2003, approximately one third of all major Internet-connected DNS servers are running BIND 9. BIND 9 has proven to be much more stable and secure than BIND 8. In addition to being the first DNS software that complied with all DNS-related IETF standards, it fulfilled all the requirements for the BIND 9 project. These included improved security, portability, maintainability, and backwards compatibility with BIND 8.

Finding the Limits of BIND

Unfortunately, the project specifications for BIND 9 did not adequately address the needs of large-scale, operationally critical networks. Some features important for high-demand networks were not included at all. Other requirements set by the funders had a detrimental effect, specifically the requirements for POSIX pre-emptive multithreading and for backwards compatibility with BIND 8 and BIND 4.

From the perspective of an administrator of a large, distributed network, BIND 9 has some shortcomings:

- **Scalability.** BIND 9 scales poorly in terms of queries per second, size of zones, or number of zones. It was designed primarily to meet the needs of a mid-scale DNS system in the mid-1990s, not to address the expanded uses to which DNS is being applied.

- **Reliability.** The multifunction design of BIND allows it to be configured as an authoritative server, a caching server, or both. This results in an unnecessarily complex system. Since BIND is multipurpose, the relatively simple authoritative function is laden down with excessive code, which impacts reliability. Though also an issue in BIND 8, it is exacerbated in BIND 9 because of BIND 9's preemptive multithreaded architecture.

- **Security.** Since BIND 9 can be used as a multifunction server (simultaneously authoritative and caching), many administrators set up their DNS servers this way. DNS experts recommend against running DNS servers as multifunction to prevent cache poisoning, which can lead to serious security breaches.

- **Performance.** The DNSSEC extensions to DNS allow cryptographic authentication of DNS data. When these are enabled in BIND 9, performance degrades to a point that some administrators would rather not enable DNSSEC. In part, this performance impact is due to fluctuations in the DNSSEC drafts while BIND 9 was being written. In any event, it creates an unacceptable tradeoff between performance and security.

- **Antiquated administration.** For backwards compatibility, BIND 9 administration is essentially the same as in BIND 8. Effectively, BIND administration has not been meaningfully updated since it was invented two decades ago. Though the software is free, managing BIND servers requires significant amounts of time from system and network administrators. The DNS protocol is complex, the BIND configuration syntax arcane. Missing semi-colons, transposed numbers, incorrect line breaks, and a host of other syntactical errors can wreak havoc on BIND servers. Even the most highly skilled (and highly paid) administrators can have problems keeping BIND error-free. Realizing you have a problem can take hours or weeks. Fixing problems can take even longer, as the DNS is a distributed database and erroneous data can live for a very long time. As a result, many network managers feel that BIND, even though free, is not cost-effective.

- **No enterprise support.** Administrators at Global 2000 companies need an enterprise-class IP name and address infrastructure that allows them to manage hundreds of DNS and DHCP servers and hundreds of thousands of IP names and addresses. This was beyond the scope of the ISC and its funding organizations.

Delivering Our Expertise

After donating BIND 9 to the ISC for distribution, Nominum worked closely with our Global 2000 support and consulting customers, and soon learned what they needed from a DNS server and what type of relationship they wanted with their DNS software provider. It became obvious that BIND 9 did not and could not meet all of their needs. Even a major update would not be enough to overcome the limitations of BIND 9 inherent in its design. We realized that yet another DNS implementation would have to be specified, designed, written from scratch, tested, and deployed.

Though several vendors successfully create and support complex open source software, we determined that Nominum could not remain viable and satisfy our customers under that model. We expanded our board of directors and, with customer data to validate the market need, received venture capital from premier investors. With over $25 million in financing to date, we transformed ourselves into a commercial software company, complete with our own project management, marketing, and sales teams.

We have not abandoned the open source community, and are still listed as an ISC development partner. Nominum engineers continue to donate code to BIND 9. There is no question that we learned many lessons while writing BIND 9. We also benefit from the decades of experience that our people bring to Nominum. Our expertise is broad and deep, and goes far beyond our experience writing BIND 9. Unlike some "younger" companies, Nominum can creatively apply knowledge gained ten or twenty years ago to solving new and emerging problems.

Nominum® Foundation™ Product Suite

Nominum's first commercial products were new, high-performing, scalable DNS protocol engines. True to our heritage, they comply with all IETF standards for the DNS protocol, including IPv6 support, DNSSEC, EDNS[4], Dynamic Update, NOTIFY, and IXFR[5]. However, our architecture is completely different from any version of BIND.

We've split DNS functionality into two servers: Nominum Foundation ANS for authoritative-only servers, and Nominum Foundation CNS for caching name servers. Each server is optimized for its dedicated function, which decreases its complexity, increases its reliability, and removes the overhead of extraneous features. Each stands alone, but can interoperate with BIND or other DNS servers. The Foundation ANS and Foundation CNS engines offer exceptional capabilities:

- **Reliability.** Foundation ANS was the heart of a DNS hosting service provided by Nominum during 2001 and 2002. For a one-year period, Foundation ANS ran with 100% DNS availability. During those 12 months, there was no scheduled downtime, and no unscheduled downtime. The DNS service was always available.
- **Performance.** Foundation CNS outperforms BIND 9 by as much as an order of magnitude. Rick Jones of Hewlett-Packard found that, on a popular HP server, Foundation CNS can handle approximately 60,000 queries per second, whereas BIND 9 handles only around 7,000 (while BIND 8 tops out at about 13,000) [6]. In addition, the Foundation servers were designed to handle DNSSEC without incurring egregious performance penalties. As a result, for DNSSEC-protected data, the performance advantage over BIND 9 is even greater.
- **Data Scalability.** Nominum's protocol engines can scale beyond virtual memory. Foundation ANS stores data in a high speed commercial embedded database, giving it the flexibility to work in extremely demanding environments without requiring huge amounts of memory. The world's largest zones can be served by Foundation ANS.
- **Manageability.** One of the major failings of BIND is that the server "goes deaf" during a reconfiguration restart. Foundation servers continue to serve their DNS zones during reconfiguration. They also support full remote configuration and operation through the Nominum Command Channel – a proprietary out-of-band protocol that allows administrators to perform such actions as creating and/or removing zones, restarting the server, and modifying DNS views. (Another Nominum product, Foundation Management Center, can provide centralized control of an entire heterogeneous constellation of DNS servers, including not only

[4] Extended DNS

[5] Incremental Zone Transfer

[6] ftp://ftp.cup.hp.com/dist/networking/briefs/lp2kr_dns_server_results.txt

Foundation ANS and CNS, but also BIND and other servers. BIND can be made more manageable with a proper management interface, but support for on-the-fly reconfiguration cannot be added without re-working the architecture of the server.)

- **Integration.** Both Foundation DNS servers coexist and interoperate with BIND 9 and other DNS and DHCP solutions. In addition, Foundation ANS uses a database back-end (with drivers available now or soon to support Oracle, Postgres/SQL, and a high-performance embedded database, BerkeleyDB). This allows Foundation ANS to be directly integrated into corporate systems. For example, a company using DNS for load-balancing could have changes in the network topology immediately reflected in the DNS data, while a service provider of IP telephony using DNS to deliver phone numbers (via the ENUM standard) could maintain the phone numbers in their current database.

After developing Foundation ANS and Foundation CNS, we further expanded our scope and developed a complete product line called the Foundation IP Address Suite. In addition to ANS and CNS, the suite includes:

- A DHCP server with IETF failover and instant restart capabilities: Foundation Dynamic Configuration Server (Foundation DCS)
- An enterprise-class IP address management application: Foundation Management Center
- An IP asset discovery and diagnosis service: Foundation Discovery Center

Foundation ANS/CNS and BIND at a Glance

	Foundation ANS/CNS	BIND 9
Performance	60,000 Queries per second (CNS); DNSSEC has minimal impact (Both)	7,000 Queries per second; DNSSEC has major performance impact
Scaling	Unlimited; Uses both memory & database	Limited to available memory
Management	On-the-fly reconfiguration; Centralized console for full remote reconfiguration and management; User friendly GUI	Reconfiguration requires restart – server 'deaf' while restarting; Management by configuration file; Limited remote management
Integration	Backend databases	None
Support	Full commercial product. Training. Bug fixes.	Third-party contractors. Self-maintenance.

Coexistence and Integration

Regardless of its limitations, BIND 9 is a high-quality DNS server that can be broadly deployed to meet specific needs. It is an excellent companion to Foundation ANS and CNS servers.

There are several reasons you might use BIND 9:

- Inertia. For many organizations, BIND 9 is already installed and meeting demand. As mentioned earlier, one third of all Internet-connected DNS servers run BIND 9.
- Cost of entry. As free software, BIND has the lowest possible cost of entry, although there may be high on-going costs to maintain anything but the simplest configurations. However, for some organizations, minimizing the acquisition cost of software is more important than reducing the lifetime cost of administration.
- Code diversity. A well-devised attack against one brand of DNS server easily spreads to other servers with the same code base. For redundancy and failover purposes, Nominum runs a mix of both BIND 9 and Foundation ANS and CNS, and recommends that other organizations take a similar approach to code diversity.

To address the challenges of managing BIND, Nominum is updating the Foundation Management Center to integrate with and manage BIND 9, recent versions of BIND 8, Microsoft Active Directory and other popular DNS and DHCP implementations. This will make it even easier to administer heterogeneous DNS environments, an important contributor to DNS reliability. In addition, Foundation ANS and DCS will be updated to support secure dynamic updates to and from Microsoft Active Directory.

Conclusion

Nominum engineers wrote two generations of DNS servers: BIND 9, which was written to replace BIND 8, and Foundation ANS and Foundation CNS, authoritative and caching DNS engines that are optimized for high-demand networks. All servers are IETF-compliant and coexist in a heterogeneous environment.

BIND 9 is a high-quality DNS server. The ISC worked with many parties, including the US Dept. of Defense and major Unix hardware vendors, to fund the project and specify the requirements, constraints, goals, and features of BIND 9. The release of BIND 9 was an important milestone for the DNS, as it was the first server to implement all DNS-related IETF standards. These standards, including DDNS, IXFR, Notify, DNSSEC, DNS over IPv6, AAAA, DNAME, and so on, are essential to support the proliferation of IP-connected devices and to support new uses for the DNS such as ENUM and Opportunistic Encryption.

Foundation ANS and Foundation CNS are stand-alone authoritative and caching DNS servers written completely from scratch. They have no code in common with any other DNS implementation. Like BIND 9, they comply with all IETF standards, and coexist with other IETF-compliant DNS and DHCP servers. They were designed from the start to meet the needs of the larger zones and organizations, to provide exceptional performance, security and scalability, and to be much easier to administer and maintain than the BIND family.

Compared to BIND 9, the Foundation DNS engines offer superior reliability, manageability, security, performance, and scalability.

Nominum encourages every organization to diversify the DNS implementations it runs for security reasons. We believe that a well-managed environment that combines Nominum Foundation DNS engines with dedicated-to-function (authoritative or caching, never both) BIND 9 servers provides the greatest resistance against possible attacks. Depending on BIND 9 as a sole solution exposes organizations to unnecessary risk. Furthermore, BIND 4 should never be used, and BIND 8 should be replaced as soon as possible.

Nominum offers a complete portfolio of enterprise-class products and services that can help network managers modernize their DNS infrastructures. These products coexist and interoperate with BIND, for greater reliability and manageable growth.

About Nominum

Nominum is a pioneering provider of IP address infrastructure software for enterprises that require reliable and secure DNS, DHCP and IP address management for their mission critical networks. Nominum is driving the future of IP addressing. For more information about Nominum, go to www.nominum.com.