



Getting Underway with ENUM: Building a DNS Infrastructure for the Convergence of Telecommunications Networks

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

www.nominum.com



Contents

Executive Summary 1

ENUM Background 1

ENUM in Action Today..... 3

The Role of DNS in ENUM..... 5

DNS Requirements for ENUM 7

Scalable Performance 8

Scalable Management 9

Security 10

Nominum Navitas 12

Summary 13

About Nominum..... 14

Executive Summary

ENUM is a combination of IP-based technologies designed to map the global Public Switched Telecommunications Network (PSTN) telephone numbers, known as E.164 identifiers, into domain names. ENUM facilitates the convergence of the Internet with traditional telecommunications services. With the increasing interest in Voice over IP (VoIP), Fax over IP, Video over IP, and other telecommunication services implemented over the IP networks, many communications companies are deploying ENUM or ENUM variations.

By implementing ENUM, communication service providers can leverage the existing base of PSTN telephone numbers and users while leveraging the cost benefits and service possibilities of packet-switched IP networks. Linking voice users with IP-based services will accelerate network convergence and the adoption of new services integrating voice and data.

ENUM relies on the Domain Name System (DNS) to distribute data about subscribers' services. But ENUM has unique requirements for the DNS infrastructure, partly because of the volume and type of data, and partly due to the service level expectations of customers used to PSTN performance. When deploying ENUM, you need DNS servers capable of delivering the scalable performance, always-on availability, rock-solid reliability and in-depth security required for carrier-class voice service.

This paper provides an overview of ENUM technology and the requirements ENUM places on the underlying DNS infrastructure. This paper is targeted to network architects, administrators and others interested in the critical infrastructure needed for telecommunications network convergence.

ENUM Background

The accelerating adoption of VoIP technologies raises interesting questions about call routing. VoIP calls use IP networks, which direct traffic ultimately using IP addresses. In contrast, most telephone users are accustomed to using unique phone numbers to place voice calls. With traditional phone routing, people are also accustomed to always-on, low-latency connections. As VoIP proliferates, how do traditional and VoIP call routing architectures coexist, without generating confusion among consumers and business users alike?

ENUM represents an effort to integrate IP telephony with traditional call routing using the globally-recognized convention of telephone numbers. Briefly, ENUM is an IETF standard for mapping unique telephone numbers (E.164 identifiers) to domain names. For detailed information on ENUM, see RFC 3761, which revised the original RFC 2916.

The beauty of ENUM is that it simplifies deployment of telecommunications infrastructures by marrying two well-established conventions:

- E.164 phone numbers (such as +1 212 555 1212 for a US number)
- The Domain Name System (DNS) – the system in use in today's IP networks for mapping domain names like `www.nominum.com` to IP addresses such as

81.200.68.204 and vice versa. DNS provides information for e-mail routing and other services

Using E.164 phone numbers allows ENUM to work within today's processes for assigning and managing phone numbers as well as facilitating the use of "legacy" devices which have limited mechanisms for data entry. Using the domain name system provides all of the benefits of DNS, including:

Scalability: The domain name system is a massively distributed database that handles millions of transactions per day. The DNS infrastructure is globally distributed, proven, and can be extended incrementally as the need grows to support name/address translations for services such as VoIP call routing.

Open architecture: The domain name system is built on open, published standards. Companies can deploy and maintain authoritative name servers, maintaining complete control over their published subscriber information. The DNS can span both public and private spaces; most companies maintain internal or private domain names in addition to those names made available to public networks.

Extensibility: Originally designed to simply map names to addresses and replace earlier, manually-maintained host tables, the domain name system has been extended many times to support new protocols and types of traffic. It can be extended anew to include service information for VoIP, Voice Protocol for Internet Mail (VPIM) and other IP-based services.

Mature functionality: In use and development for two decades, DNS has a rich set of features, including data replication, data caching, cryptographically strong security, and dynamic updates. These features are essential to providing high levels of availability, performance, security and manageability.

But perhaps the greatest advantage for carriers using ENUM is the potential cost savings of an IP-based infrastructure over a PSTN TDM-based infrastructure. To leverage the full benefits of these cost savings, you must build the ENUM infrastructure to handle expected query and update demands efficiently and effectively, while maintaining the service levels that subscribers demand.

Some ENUM Terminology

| | |
|-----------|--|
| VOIP | Voice over IP |
| IETF | Internet Engineering Task Force – a standards body defining Internet protocols |
| ENUM | An IETF standard originally defined in RFC2916 for associating telephone numbers to domain names and service information |
| ITU | International Telecommunications Union |
| PSTN | Public Switched Telephone Network, the global voice telephony network |
| E.164 | The ITU standard for the PSTN describing telephone numbers, such as +1.650.381.6000 or +44.7703.649313 |
| E164.arpa | The root domain for public ENUM implementations |

ENUM in Action Today

ENUM was intended to create a global, public telephone number directory in the domain name system, with each country managing registration for its own country code within the E164.arpa domain. This effort is underway today, with field trials ongoing in several countries. Some countries, such as Austria, have already implemented ENUM for public use. But global success for public ENUM entails resolving political, legal, organizational and logistical challenges.

Many telecommunications companies and multi-service operators (MSOs) are looking at implementing private or carrier ENUM, in response to growing competition in providing VoIP and other messaging services. Although these projects are outside of public ENUM and the telephone numbers would not be mapped into the E164.arpa domain, they share the technological attributes and conventions of public ENUM.

There are many terms used to refer to these different types of ENUM implementations, including infrastructure ENUM, carrier ENUM, golden tree and silver tree ENUM, etc. For the purposes of this paper, we will differentiate them as follows:

Public ENUM Tiers

| | |
|--------|--|
| Tier 0 | The root level ENUM, managing e164.arpa, currently managed by the ITU and RIPE NCC. |
| Tier 1 | The country-level registries of ENUM information. |
| Tier 2 | Registrars within each country code. These might be organized by prefixes, regions, or other attributes. |

| | |
|--------------|--|
| Public ENUM | <p>The public, global ENUM directory has the goal of being universally available, translating telephone numbers into domain name strings for subsequent DNS queries within the E164.arpa domain.</p> <p>As its name implies, public ENUM data will be publicly accessible. As with the existing telephony system, a global public directory of subscribers will connect telephone numbers with other communication services. The data will be accessible using the E164.arpa domain at the public DNS root, and, in theory, subscribers should be able to edit service information associated with telephone numbers assigned to them.</p> |
| Private ENUM | <p>In a private ENUM deployment, the DNS services for the ENUM project are internal to a telecommunications organization's internal namespace. For example, a carrier might use private ENUM for all users within the company's voice plan. Or, a mobile operator could use ENUM to route Multimedia Messaging Service (MMS) traffic between phones within its domain. Many carriers are deploying private ENUM implementations as internal pilots before undertaking larger efforts. The mapping and service data used within a private ENUM deployment is not publicly available.</p> |

| | |
|--------------|---|
| Carrier ENUM | Carriers are also using ENUM to route message traffic between multiple carriers without going through the PSTN. The term "infrastructure ENUM" is sometimes used to refer to these types of ENUM services between carriers and outside the E164.arpa root domain. As with Private ENUM, the mapping and service data used within Carrier ENUM deployments is not publicly available, but is instead accessible to the participating carriers. |
|--------------|---|

Public, private and carrier ENUM will coexist for some time. Many providers creating private ENUM deployments, while others are using carrier ENUM deployments with other carriers to support VoIP peering, routing VoIP calls entirely over IP networks.

ENUM has many potential uses, such as routing IP-based traffic for MMS and SMS services, interconnecting various Internet-based services with the PSTN, and providing PBX-like functions such as call forwarding to Internet-based communication services.

Whether you are looking to do a private implementation, participate in the public ENUM process, or exchange VoIP peering information using carrier ENUM, a robust, reliable, highly available, high performing, scalable, and secure DNS infrastructure is required to handle the demands ENUM places on the DNS.

The Role of DNS in ENUM

ENUM technology uses the Domain Name System (DNS) to store and serve the information linking phone numbers to network addresses and services.

- An ENUM-compliant client device (such as a phone or a VoIP PBX) translates the phone number into a domain name by reversing the digits and putting periods between each, and adding the appropriate zone information. For public ENUM, all numbers will be placed into the E164.arpa domain.

For example, the phone number
 +1 234-567-8901
 becomes:
 1.0.9.8.7.6.5.4.3.2.1.E164.arpa

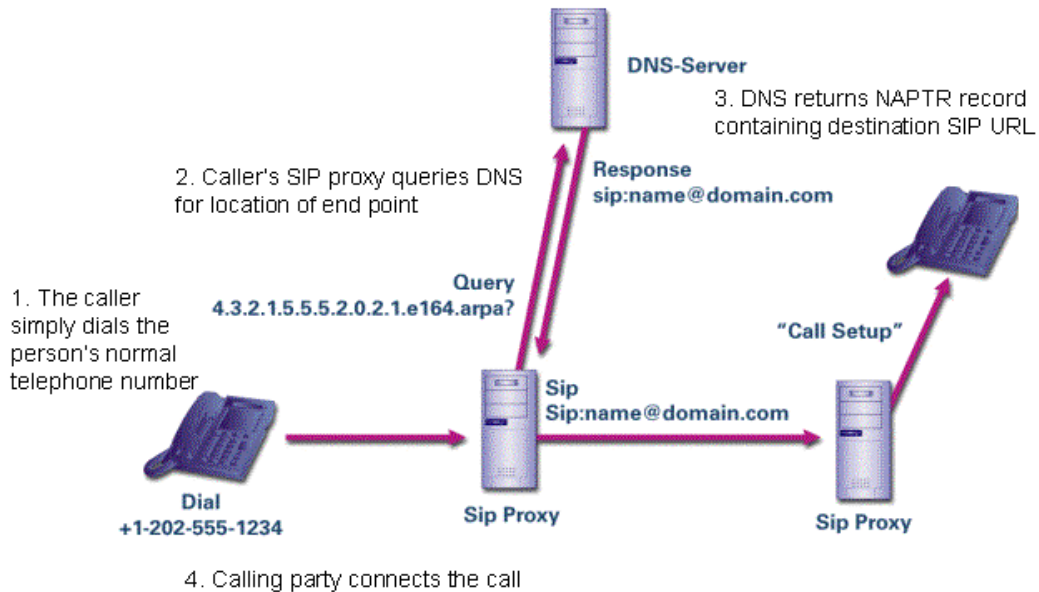
- The client device queries a *caching name server* with the transformed telephone number, asking for all Naming Authority Pointer (NAPTR) resource records associated with that telephone number. If the caching server doesn't have that data locally (if it hasn't asked the same question recently), it will find and ask an authoritative name server for the NAPTR records in the appropriate ENUM domain, returning this information to the client device.
- An *authoritative name server* contains the ENUM data or referrals to other name servers which contain the ENUM data. In Public ENUM, the E164.arpa domain contains referrals pointing to other authoritative name servers which serve the E.164 "country codes" (e.g., "1" for the North American Numbering Plan, "4.4" for the United Kingdom, "1.8" for Japan). How domain name delegations occur within a country code is entirely determined by the delegation-receiving organization in the ITU member state. Some member states may, for example, have no sub-delegations, having instead a single zone for all telephone numbers within their country code. Other member states may decide to partition their ENUM space according to regional "area codes". If and how the partitioning occurs is the responsibility of the organization to which the country code delegation is made.
- Within the DNS, a set of NAPTR resource records contain information about services available to that number. For VoIP, that information might include the addresses of SIP or H.323 services.

DNS and VOIP Terminology

| | |
|-----------------------------------|---|
| Authoritative name server | A DNS name server hosting the authoritative data for a domain name zone. |
| Caching name server | A DNS name server that responds to client queries, retrieving and caching information from authoritative servers. |
| NAPTR (Naming Authority Pointer) | A resource record within the DNS information that can contain information about services |
| Resource Record (RR) | A record within a Domain Name Server that describes an Internet resource. The NAPTR is one type of resource record. |
| H.323 | ITU's signaling protocol for VoIP |
| SIP (Session Initiation Protocol) | IETF's signaling protocol for VoIP |
| Zone | A unit of DNS administration: the part of the DNS over which an administrator has edit control. |

- On the client device, an “ENUM Resolver” is responsible for processing the NAPTR Resource Records (RRs) and using the information delivered in the DNS record to establish the appropriate form of communication.

The following figure shows the simplified flow through the DNS for setting up an SIP call:



The basic ENUM architecture can provide accessibility to many services from legacy devices via the DNS architecture, linking all kinds of IP-based services beyond simple voice telephony to a telephone number, including:

- E-mail
- Faxes
- Instant Messaging
- SMS (Short Message Service)
- MMS (Multimedia Messaging Service)

ENUM uses the NAPTR resource record to store information about which of these services is available for each phone number. In many cases, the exact data stored will depend on what the user chooses to make available. For example, in some deployment scenarios, users can gain access to their ENUM NAPTR records directly, allowing them to specify that a MMS message should be sent to Mobile Phone operator A, an instant message should be sent to computer B, and voice telephony to SIP proxy C.

NAPTR records can include other information, such as the “preference order” for various services. These preference orderings can be used to offer enhanced availability of service

and to balance load between servers. NAPTR resource records can also be used to specify a transformation of an input string, such as a userid, into an output string. This flexibility ensures that you can extend the basic ENUM architecture as new technologies come along, “future-proofing” the deployment of ENUM-based infrastructure.

DNS Requirements for ENUM

All you need to start using private or carrier ENUM is a DNS infrastructure to publish and fetch the NAPTR information associated with a set of telephone numbers and a means of populating and managing that information. At the bare minimum, this means an authoritative DNS server to publish the ENUM information, and caching DNS servers to give clients access to that information.

In designing an ENUM trial or initial implementation, you should deploy a DNS infrastructure that will be able to support the longer-term attributes of ENUM and VoIP call routing. It is tempting to use open source or other freely-available DNS servers to support ENUM field trials or implementations. However, as usage inevitably grows, it is extremely likely you will find yourself struggling to maintain service levels and meet performance and availability requirements. As the ultimate object is to provide at least the same quality, availability and performance of traditional telecommunications networks, it is not enough to simply make ENUM “work” – it has to be viable in the context of the two inevitable trends in network convergence: growth in customers and services and increased dependence upon those services.

Preparing for growth

The ENUM infrastructure must be massively scalable to handle growing numbers of entries as well as queries against those entries. ENUM information will change frequently. Even today, DNS content changes have to be globally available almost instantly to meet service level agreements, so it is important to base your infrastructure on a DNS server that is able to handle a high rate of DNS updates. As technologies that can make use of ENUM such as VoIP proliferate, either within your network or between networks, more of the call or connection setup and routing traffic will travel over the Internet and use ENUM-based lookups.

This inevitable growth drives specific DNS requirements:

- Scalable performance under large query loads. Any latency in query response creates a delay in establishing a call or connection. PSTN call establishment is expected to take less than 200 milliseconds, so this must be the upper bound of ENUM based lookups regardless of the amount of data the DNS server is offering or the query load the DNS server is experiencing. This low latency query response must be consistent under load and during data updates.
- Scalable management. As the amount of data under management grows, telecommunications providers need the ability to add, modify, or delete the data in real time with no interruption of service, and to integrate the ENUM data management into existing provisioning processes. Failure to do so increases the overhead of managing the ENUM data and can add undue costs, delays, and service interruptions, eroding some of the benefits and efficiencies the converged networks can provide.

Preparing for increased dependence

Just as inevitable as the growth of the converged of voice and data network components is the increased dependence upon the infrastructure underlying the converged network. Although today most organizations maintain separate equipment for voice and data, convergence is exposing voice, video, and other traffic to some of the risks present in today's data networks.

The ENUM infrastructure, available to external data networks, offers a point of vulnerability in converged services. The DNS infrastructure hosting ENUM must help protect the security and privacy of data. While the disruption of the Internet for electronic commerce can be extremely expensive, the disruption of telephony can have fatal consequences. This fact demands selecting DNS servers that provide very high availability and reliability as well as resilience to a variety of Internet-based attacks.

The following sections describe the performance, management and security requirements in more detail.

Scalable Performance

The first step is to estimate the amount of data to be served in an ENUM DNS server and the peak lookup volume against that data. When considering these estimates, plan for long-term deployment rather than limited trial conditions and provide for sufficient "breathing room" to anticipate reasonable unexpected growth. In other words, double or triple your best estimates of both data and lookup quantities. As we will see in the sections that follow, scalability has significant implications for security and availability.

Scalability has many dimensions; when considering DNS servers, you need to consider the following:

- The size of the DNS zones; the ENUM server may host tens of millions of records or more, and NAPTR records for ENUM can be significantly longer than standard DNS records.
- The amount of queries per second the server can process; in some DNS implementations, the number of queries per second degrades considerably with larger zones.
- The overall query latency, or the time it takes to respond to a single request. For PSTN call establishment, this should be less than 200 milliseconds. As an ENUM resolution may take multiple queries, a much lower query latency (<1 millisecond) is ideal.

When considering the DNS server to use, a variety of options present themselves. Many, if not most, initial trials of ENUM technology were based upon the Open Source BIND version 9 DNS server available from the Internet Systems Consortium. This server was designed and written by Nominum as a proof of concept reference implementation of all the DNS protocol specifications, including several protocol features that have since been deprecated or revised. BIND version 9 was not explicitly architected with carrier-grade services in mind. It is a multifunction server, offering both authoritative and caching name server capabilities without being optimized for either. While BIND 9 is generally

useful for many applications, it has significant limitations when considered as a basis for carrier-class services.

For example, BIND stores all DNS data in memory, loading the data from an ASCII text file on server startup, reconfiguration, or reload. During startup or reconfiguration, the BIND server is unable to answer any queries. When reloading a particular zone, BIND is unable to answer queries for that zone. As the amount of data being managed grows into the millions of telephone numbers, this design imposes unacceptable limitations:

- The amount of physical RAM on the server creates a fixed limitation for the amount of data an authoritative server can publish. If you have millions of records, you will need tens of gigabytes of high speed ECC RAM to provide any DNS service. (If BIND exhausts memory when loading data, it crashes.)
- Because data is loaded into memory on the server start, you must either reload the zone or the server when modifying DNS data or you must use the DNS Dynamic Update protocol. This load time is proportional to the amount of data; the more data you have, the longer it will take to load the server. If you are using Dynamic Update, the data you can modify is limited in terms of quantity, and there are specific limitations on what data can be deleted.
- Restarting BIND takes the server offline for a period of time relative to the amount of data. This impacts availability and performance.
- The internal data structures of BIND were optimized for limited data quantities. As the amount of data increases, the amount of time to search through that data also increases. Thus, when a server is loaded with millions of records, the response to all queries slow down significantly.

The ENUM infrastructure should be able to respond rapidly to large numbers of queries, minimizing latency when initiating a connection such as a VoIP call. You should be able to handle growth without a proliferation of servers to manage. Although the software for BIND servers may be free, the savings on commercial software can easily be offset by hardware and operational costs as well as management overhead of supporting many DNS servers.

Scalable Management

Scaling the ENUM implementation presents management challenges as well. To achieve the cost efficiencies promised by packet networks, you need the ability to update and manage the ENUM infrastructure in real-time, without outages.

Large, real-time updates

The first requirement is the ability to update ENUM information while it is live. You need to add, modify and delete data in an environment with high, continuous query loads, without degrading performance.

A production ENUM system must handle large numbers of updates per second – either due to multiple people requesting changes or service updates for blocks of numbers (such as a corporate customer). Many large updates must be implemented atomically (either in entirety or not at all) to ensure data consistency.

There are two ways to manage updates to DNS systems – using the DNS server’s internal configuration mechanism, or using the DNS protocol itself (the dynamic update feature).

- Dynamic update has limitations; there are operations you cannot do with the dynamic update protocol, like delete an entire zone. And the dynamic update itself is limited to 64K of data, which means that larger updates must be split up. Splitting large updates can create data consistency problems.
- For large updates, therefore, it is often better to update the DNS server directly. For BIND servers, this means waiting while the server reloads a zone or its data, which is unacceptable in a high volume production environment.

Integrating Updates with Provisioning Systems

As long as updates require manual, expert intervention, they will be expensive and error-prone to deploy. By integrating updates with provisioning systems, you can reduce the “change latency” of implementing or changing services, while reducing the potential for human errors.

To be efficient and competitive, service providers need ENUM solutions that let the subscriber change their own NAPTR records at a self-service portal. For example, an authenticated user would initiate the change at a portal, and then a back-end system would validate the change and communicate with the ENUM server to enact the real-time update.

From the DNS server perspective, these functions drive the following requirements:

- High performance, even under high query and update loads.
- Reconfiguration of data and zones on the fly, without outages or restarts.
- APIs for integration with provisioning and user update systems

Security

In data networks, the DNS infrastructure has proven to be a target for numerous attacks on network services or data. By shutting down DNS services, attackers can disrupt network access for large numbers of users. Because ENUM uses the basic DNS infrastructure, it is vulnerable to the same risks. Security is a particular issue for public ENUM, although even private and carrier ENUM implementations can be affected by worm- or virus-related traffic that overwhelms the server.

Although there are many potential risks to DNS public servers, they can be grouped into a number of categories: data integrity attacks, denial of service attacks, and registry attacks.

Data integrity attacks, such as spoofing and cache poisoning, enable attackers to pretend to be someone they’re not. You can alleviate these risks by verifying the authenticity of ENUM data using security mechanisms.

The DNSSEC extensions to DNS integrate public key cryptography and digital signatures to authenticate the origin and integrity of DNS data. But DNSSEC increases the size of the response packets, and degrades the performance of public domain BIND servers

(ironically increasing their exposure to Denial of Service attacks).

In addition to high performance, using DNSSEC requires effective management tools. For example, you need the ability to “sign” zones offline, outside of the running DNS server, then switch over to the new, signed zones.

For ENUM implementations, DNSSEC requires the participation of the parent zone. The performance issues and the need for a critical mass have slowed adoption of DNSSEC in the Internet at large. However, in private and carrier ENUM deployments, with known DNS servers hosting ENUM data, DNSSEC deployment may be practical.

Denial of Service attacks flood DNS servers with malicious queries until they cannot respond to legitimate queries, often by enlisting hijacked or “zombie” computers. A distributed DOS attack may increase the DNS traffic volume by several orders of magnitude.

Worms and viruses can also generate large amounts of spurious traffic in seeking to propagate themselves. These DNS lookups effectively function as a denial of service attack, overwhelming DNS servers and disrupting service for legitimate requests.

These problems are best countered by maintaining enough spare capacity in the DNS servers to handle a tremendously increased query load without failure.

Internet specification RFC 2870 suggests that as a best practice, critical DNS servers should maintain the capacity to handle three times the current peak load in normal situations. To achieve the kind of reliability that users expect from a traditional switched telephone service, authoritative servers hosting ENUM data should adhere to similar rigorous standards, maintaining sufficient overhead to absorb significant, malicious spikes in traffic.

Registry attacks occur when someone convinces an operator to incorrectly update DNS registry information. Although the target is the DNS data and the attack may be publicized as a failure of the DNS information, the attack is most often a social engineering one, and thus difficult to defend within the DNS server. As with most security issues, the biggest risk is the human factor.

ENUM Server requirements

How do these security issues translate into DNS server requirements for ENUM implementations?

- DNS servers filling ENUM roles should support DNSSEC without significant performance degradation, and have the ability to manage DNSSEC updates. They should also standards such as TSIG (Transaction SIGNatures), which secure the authenticity of the sender of an update and vice versa.
- The ENUM infrastructure should have the extra capacity to handle a significant increase over peak query loads.
- Both authoritative and caching DNS servers should use software without known, published vulnerabilities – the latest versions of open source or commercial implementations.

“Finally, as an ENUM service will be implementing some type of security mechanism, software which implements ENUM **MUST** be prepared to receive DNSSEC and other standardized DNS security responses, including large responses, EDNS0 signaling, unknown RRs, etc.”
RFC 3761

Nominum Navitas

Nominum has created a carrier-grade, ENUM-based directory server of addressing the demands of ENUM operations in next-generation networks.

Nominum Navitas leverages existing DNS and ENUM standards to create a lightweight, highly scalable and flexible directory for IP-application routing information, linking services to subscriber names or phone numbers. Navitas supports VoIP as well as all kinds of advanced services.

Navitas addresses the stringent requirements for scalability, performance, manageability and security in communications networks.

- Navitas uses data structures and patent-pending data compression optimized for NAPTR data supporting ENUM. As a result, it is able to handle very large data volumes (hundreds of millions of records.) It also offers flexible and innovative zoning structures to manage those large amounts of data efficiently.
- The product supports real-time bulk or incremental updates through a number of open provisioning interfaces, including an Extensible Provisioning Protocol (EPP) interfaces using SOAP/XML. Nominum also supplies packaged connectors for third party service bureau and other data sources, such as Neustar.
- An integrated element management system (EMS) helps network operations centers maintain optimal services levels and responds to potential problems on the ENUM server quickly.
- Navitas protects the security of ENUM data through supported protocols like DNSSEC and TSIG. It uses no open source code with known, published vulnerabilities. In addition, the inherent scalability of the Navitas engine lowers the possibility that a Denial of Service attack can successfully degrade service.

Finally, Navitas offers the highest levels of throughput and lowest latency for large data volumes. In tests designed to replicate the potential long-term requirements for production ENUM applications, Navitas has demonstrated the ability provide highly scalable performance.

For example, Nominum tested the Navitas server with a load representative of production carrier environments: 200 millions records, 30 updates/second, serving simultaneous queries. The results were as follows:

| | Nominum Navitas |
|-----------------|-------------------------------|
| Memory required | 3G (for 200 millions records) |
| Average latency | < 1 millisecond |
| Queries/second | 16,000 |



The BIND 9 serve was unable to load 200 million records, and required 32G of memory to load only 50 million NAPTR records.

Summary

ENUM will serve an increasingly important role in converging networks. It is already growing in importance due to the growth in VoIP peering efforts and the need for SMS message routing. ENUM will be an essential component of IP Multimedia Subsystem (IMS) networks, and can serve as a directory for routing all kinds of advanced services in next-generation networks.

When building your ENUM solution, whether for a major production implementation or initial trial, keep the long-range needs for scalability, manageability, security and performance in mind. Nominum Navitas is a long-term solution for handling ENUM directories. It has the flexibility and open interfaces to adapt to a wide range of systems. Security, element management and administrative interfaces help Navitas integrate easily into carrier network operations. And Navitas can support the enormous data volumes, update requests and performance requirements of carrier environments.



About Nominum

Nominum's network naming and addressing solutions power the world's largest always-on networks. Nominum is a global provider of ENUM-based IP-application routing directories, DNS, and DHCP solutions that enable communication providers to deliver high quality always-on broadband internet and innovative services to their customers, including VoIP, push to talk, fixed-mobile convergence, IPTV, and triple-play.

For further information, visit www.nominum.com.