Company Overview

An industry leader and pioneer in Managed DNS Services

• **UltraDNS acquired by NeuStar, Inc. (NYSE: NSR) in April 2006**
  – UltraDNS technology and solutions part of NeuStar Ultra Services (NUS)
  – Thousands of customers worldwide
  – Significant penetration among Fortune 1000 and Service Provider sectors

• **Leading DNS provider to the Top-Level Domain (TLD) community**
  – Infrastructure provider for over 30 cc, s, and gTLDs
  – Manages approximately 25 million domains, over 20% of global domain market
  – Network processes in excess of 175 billion queries per month

• **NeuStar provides full service registry solutions**
  – SRS
  – Registry Gateway
  – Whois
Legacy DNS Vulnerabilities

- **Decentralized nature of DNS hierarchy vulnerable to attacks**
  - Attacks launched against critical control points (i.e., root servers, TLD’s) create wide-spread outages
  - If DNS does not function, users will never reach intended content

- **DNS is ‘weak link’ of the Internet but critical component of advanced applications**
  - VoIP / ENUM
  - RFID
  - E-commerce

- **No out of band ‘command and control’ in DNS**
  - Effectiveness of infrastructure can easily be interrupted by public users of the system

- **BIND software ranked as top security vulnerability on the Internet**
  - SANS Institute:  [http://www.sans.org/top20/](http://www.sans.org/top20/)
  - CERT advisories

- **DDoS attack patterns becoming more sophisticated and effective**
  - Internet root servers in November 2002
  - Akamai outage in July 2004
  - Distributed reflector denial of service attacks in January 2006
  - Internet root server attack in February 2007
  - Attack against Estonia in April 2007 – first cyber attack against a country
## NeuStar Ultra Services

### Value Propositions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td>Proprietary non-BIND software; provides code diversity</td>
</tr>
<tr>
<td><strong>Service Guarantee</strong></td>
<td>Includes SLA with 100% uptime network guarantee</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Faster customer connections via routing to closest topological server in global network; real time replication of DNS changes</td>
</tr>
<tr>
<td><strong>Management Tools</strong></td>
<td>XML API or intuitive web-based GUI to centrally administer DNS settings using role-based security</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Protects from hacker attacks including DDoS&lt;br&gt;Secured access to NeuStar Ultra Services nodes and name servers</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Leverages DNS infrastructure on 5 continents to scale globally</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>24x7 proactive support</td>
</tr>
</tbody>
</table>

**No additional hardware, software, maintenance or training costs**
Intelligent Routing
IP Anycast

• **Pioneered IP Anycast for directory services**
  - Provides redundancy and efficiently utilizes system resources for maximum scalability

• **IP Anycast and BGP routing**
  - Failover & self-healing capabilities allows NUS to add or remove servers with no user impact
  - Queries directed and processed by the topologically closest server

• **Protects network from DDoS attacks**
  - Methodology sinks DoS attacks at source of the attack
  - Prevents customer facing issues
  - Strong relationships with upstream providers

• **Performance enhancer**
  - Mitigates delays in resolution
  - Limits number of foreign routes to traverse reducing packet loss
  - Reduces the number of query packets that are dropped and cause a DNS timeout/retry

• **Added reliability achieved by having 6 shared global IP addresses**
  - Provides additional redundancy in the face of network routing problems (e.g. black holes)
Data Propagation
Master–to–Master Replication

- **Maximum scalability and performance**
  - Two-tier replication environment
  - Numerous data triggers are designed to ensure timely cache

- **Fully redundant, scalable and fault-tolerant**
  - Utilizes a hierarchical methodology for robust replication
  - Incorporates tightly integrated code that monitors local system
  - Routing announcements immediately withdrawn upon application, server, or network failure

- **Master-to-master replication schema**
  - Replication engine interacts directly with the database
  - Maintains consistency between the information at each node in a mesh
  - Synchronized via replication over the wide area network
Current Data Centers (14)

- **North America**
  - California (3)
  - Illinois
  - Virginia (2)
  - Florida
  - Texas

- **Europe**
  - Luxembourg
  - UK

- **Australia**
  - Sydney

- **Africa**
  - South Africa

- **Asia**
  - India
  - Hong Kong

Planned Expansion
- China
- Canada
- South America
DNS Shield created to mitigate DDoS attacks launched against DNS infrastructure

- **Focus on top 20 Global ISP/network providers**
  - AOL, EarthLink, Cablevision, Qwest, Yahoo!
  - Significant ISP and network provider demand
  - Targeting to cover 75% of end users

- **Private Nodes deployed within Major ISPs/Network Providers**
  - Inaccessible to public
  - Accessible only to “trusted” recursive servers

- **Providers create and maintain Access Control Lists (ACLs)**
  - Restricts access to Ultra Service Nodes and provider’s recursive name servers
  - Forms a protected environment for DNS query and response traffic

- **Each partner deploys two or more authoritative private nodes**
  - Functionally identical to NUS Public Nodes
  - Utilizes Anycast IP addressing via BGP
  - Connected privately to Ultra Services Replication System
• A constellation of private nodes with secure links to the Ultra Services global network forms a trusted DNS infrastructure
• **DNS Shield leverages the Service Provider’s existing infrastructure**
  – No changes necessary in recursive server query lookup

• **Reduces Customer Support costs associated with effects of DDoS against DNS**
  – Without DNS Shield implementation, Service Providers must burden support costs associated with end users that cannot reach intended destination due to DNS disruption

• **DNS Shield provides increased DNS resolution performance for end users**
  – Authoritative server proximity to end users allows query response times of less than 5 milliseconds

• **Service Provider’s zones are cross-pollinated within each others infrastructure**
  – Enables DNS to function even while under a severe DDoS attack
  – End user recursive queries are completed in an isolated and trusted environment

• **Ultra Services provides code diversity and global footprint that augments existing Service Provider’s infrastructure**
Partnering with TLD Operators
Solutions Address Critical Challenges

• Advanced services viewed as critical by TLD administrators

  – DNS Shield Protection
    • TLD’s get benefit of DDoS protection on both the public and private infrastructure
    • Provides significant performance improvements in DNS resolution to each end user community even if the public infrastructure is under DDoS attack
  – DNSSEC
    • TLD’s looking towards DNSSEC as a critical security layer for protecting end user community
    • DNSSEC test-bed available to TLD customers
  – IPv6 Support
    • Network is deployed with IPv6 native connectivity to all nodes
    • Supports AAAA records
  – IDN Support
    • Network is compliant with both ASCII and Punycode
    • Single lookup supports both 8-bit and Punycode server side characters
  – ENUM
    • Ultra Services infrastructure and API compliant with NAPTR record administration key for ENUM routing
    • Production environment available to facilitate TLD adoption of ENUM services
• TLD’s can utilize NeuStar for either Primary or Secondary DNS
  
  − Over 25 node locations to serve DNS on both the public and DNS Shield networks
  
  − DNS managed via XML API or AXFR/IXFR
    • Changes propagated globally in 2 minutes or less
  
  − TLD traffic managed on separate network from enterprise customers
    • TLD network customized for processing high query volumes
    • Injection methodology designed for scale
    • Isolate effects of attack traffic from enterprise network
    • Dual GigE connections at each node, Juniper M120 carrier class routers
  
  − Detailed domain/query reporting and traffic logging for all TLD customers
    • Segmented by time of day and network location
  
  − Custom infrastructure solutions available where NUS can anycast TLD controlled IP addresses
    • Disaster Recovery solution
    • Real-time enablement of the NUS infrastructure to process queries during high volume periods
Michael Guglielmi
Michael.guglielmi@neustar.com

Neustar Ultra Services
1000 Marina Boulevard
Suite 400
Brisbane, CA 94005 USA

+1-650-228-2358

www.neustarultraservices.biz