VERISIGN® MANAGED DNS

USING HYBRID ROUTING TO OPTIMIZE DNS RESOLUTION PERFORMANCE AND RELIABILITY
EXECUTIVE SUMMARY

TO CREATE A SATISFACTORY END USER EXPERIENCE, DOMAIN NAME OPERATORS MUST ENSURE THAT DOMAIN NAME SYSTEM (DNS) RESOLUTION IS FAST AND RELIABLE. DNS QUERY ROUTING—VIA UNICAST, ANYCAST, OR A COMBINATION OF BOTH—IS AN IMPORTANT VARIABLE IN PERFORMANCE AND AVAILABILITY OF EVERY SERVICE ON THE INTERNET. IN MANY CASES, A HYBRID SOLUTION COMBINING BOTH UNICAST AND ANYCAST CAN PROVIDE THE BEST BALANCE BETWEEN TRANSACTION LATENCY (PERFORMANCE) AND TRANSACTION SUCCESS (AVAILABILITY). HOWEVER, MOST DNS SERVICE PROVIDERS CAN ONLY OFFER A STRICTLY ANYCAST OR A STRICTLY UNICAST SOLUTION. IN ADDITION, SOME PROVIDERS AND IN-HOUSE DEVELOPERS DO NOT HAVE THE EXPERIENCE, PROCESSES, OR INFRASTRUCTURE TO PROPERLY DESIGN AND EXECUTE HYBRID GLOBAL ROUTING SOLUTIONS.

VERISIGN® MANAGED DNS COMBINES IP ANYCAST AND UNICAST TECHNOLOGY TO PROVIDE A FLEXIBLE HYBRID APPROACH THAT HELPS OPTIMIZE PERFORMANCE AND RELIABILITY FOR NAME SERVER QUERIES AND RESPONSES (I.E., TRANSACTIONS). THIS ROUTING APPROACH—ALONG WITH INDUSTRY-LEADING SERVICE LEVELS—IS UNIQUE TO VERISIGN AND DIFFERENTIATES THE VERISIGN MANAGED DNS SERVICE FROM ITS COMPETITORS. USING VERISIGN MANAGED DNS, ORGANIZATIONS CAN LEVERAGE VERISIGN’S EXPERTISE AND GLOBAL DNS INFRASTRUCTURE TO ADDRESS SPECIFIC NEEDS FOR RESOLUTION PERFORMANCE, SCALABILITY, AND AVAILABILITY, WHILE

THE DOMAIN NAME SYSTEM (DNS)

As the name resolution system for the Internet, the DNS maps Internet domain names to IP addresses. Almost any device that interfaces with the Internet (e.g., computers, mobile devices, laptops, ATMs, and point-of-sale, or POS, terminals) relies on DNS services to enable information exchange.

When a user enters a domain name into a Web browser or other application, the DNS resolution process uses a globally distributed network of authoritative and recursive name servers to obtain the domain name’s corresponding IP address and then direct the user to the desired service. This network of name servers resides within the DNS ecosystem, which consists of a hierarchy of zones.
Each zone contains one or more authoritative name servers or nodes that resolve IP address requests for one or more domain names. If a recursive name server cannot resolve a query for an IP address locally or from its cache, it queries authoritative name servers to find a server that can help accomplish the name resolution task.

Virtually all Internet applications and services—ranging from Web sites, email, social networking, and online banking to voice-over-Internet protocol (VoIP), file sharing, and video on demand—depend on name servers for DNS resolution. Name server availability and the speed at which servers can receive and respond to DNS queries significantly impact the quality of the user experience.

Apart from the high-level variables—skill set, processes, and global infrastructure—that impact DNS resolution, many variables within a zone itself can influence the performance and availability of authoritative name servers. These variables include the message size of responses to DNS queries, the type of transport protocol used (e.g., User Datagram Protocol, or UDP, versus Transmission Control Protocol, or TCP), the compressibility of labels within domain names, and the number and configuration of authoritative name servers within the zone. This white paper focuses on the last variable and examines how multiple authoritative name servers—when implemented and configured appropriately—can improve both resolution availability and performance.

IMPROVING AVAILABILITY AND PERFORMANCE

To ensure that DNS queries are resolved promptly and reliably, many domain operators host authoritative name servers from more than one location (node) for a given zone.

A multinode strategy helps increase the availability and performance of the resolution process in the following ways:

- **Availability** – Multiple discrete physical nodes provide operational redundancy and help distribute query loads. Instead of relying on one server in a single data center, the resolution system is backed by multiple data centers and name servers that service each zone. Ideally, two or more data center operators and network providers are used so that at least one of the centers remains operational should a single provider experience a catastrophic failure. If one center fails or is over-burdened for any reason, the remaining node(s) can handle resolution tasks. It is important to note that the remaining node(s) must have ample capacity to absorb the additional load from any nodes that fail.

- **Performance** – A geographically distributed and topologically diverse presence increases the probability that a client system is closer to some portion of the authoritative name resolution system. The closer a client is to a node, the faster it can obtain a response to a DNS query. Close proximity to authoritative name servers can reduce transaction latency by hundreds of milliseconds.

As outlined above, during a typical attempt to resolve a DNS query, a recursive name server iteratively cycles through the zone’s authoritative name servers until it receives a response to its query. Ideally, recursive name servers route every DNS query to the node that provides the lowest transaction latency, with geographic proximity and network topology (i.e., round-trip time) influencing latency the most. In fact, most recursive name server implementations do establish varying levels of affinity for specific authoritative name servers during steady state conditions and over time. However, they are not inherently configured to factor service distribution and external routing functions, which change over time, into their server selection algorithms.

To maximize the benefits of a multinode infrastructure, domain name server operators must have the expertise, processes, and global points of presence to enable optimal servicing of requests for DNS query resolution. The two most common methods of servicing DNS queries and responses are via unicast and anycast routing.

ROUTING VIA UNICAST AND ANYCAST

At their most basic, unicast and anycast can be defined as follows:

- **Unicast** – Communication between
a single client and a single server

- Anycast – Communication between a single client and the topologically closest instance of a network service that is represented in multiple places by a common IP address

Until recently, organizations relied on one approach or the other for DNS resolution. Verisign advocates a hybrid solution that employs both unicast and anycast routing to optimize both resolution performance and ultimate service availability.

**Unicast**

With IP unicast routing, only one location services the IP address associated with a given network service. Because only one name server and one instance of the associated IP address exists in the global routing system, the routing system and network data path are less complex than an anycast system.

Because unicast is less complex, routing errors and other conflicts that interfere with DNS resolution reliability are less likely, and operators can more easily detect data path aberrations when they do occur. In addition, unicast configurations help minimize localized or regional transient network or routing system conditions that may affect system availability. For these reasons, unicast is ideal for situations that require high availability. On the other hand, transaction latency for a widely distributed set of clients may increase because only one server in one physical location is available for service distribution.

**Anycast**

IP anycasting allows a single name server IP address to exist in multiple locations at a given time. In this approach, DNS requests are routed between a single source (the client’s DNS recursive name server) and the topologically closest authoritative node. In theory, the client reaches the topologically closest anycast instance, as determined by Internet routing protocol metrics; however, all instances are configured with the same IP address and provide exactly the same service. Although anycast is ideal in environments with highly variable routing conditions and short-lived, connectionless transactions, the possibility of transient routing systems or forwarding path changes lessens its suitability for long-lived, persistent TCP transactions and similar scenarios. In all cases, anycast must be configured carefully to avoid widespread resolution failure.

**Ideal in Environments with Highly Variable Routing Conditions**

Because DNS requests can be routed to the closest server in a

---

**Table 1 – Unicast Benefits and Challenges**

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides greater stability and reliability overall by minimizing the number of server switches and unanswered queries.</td>
<td>Impacts performance by increasing latency.</td>
</tr>
<tr>
<td>Minimizes routing cost and complexity.</td>
<td></td>
</tr>
</tbody>
</table>

---

Transaction Latency

In the context of DNS resolution, performance is expressed in terms of transaction latency. In general, the transaction latency variables are forward- and return-path latency (round-trip time, or, RTT), and client/server processing. Aggregate forward (client to server) and return path (server to client) propagation delay variables, which are primarily a function of the physical-layer network path between the client and server (network proximity), and to a lesser extent nodal processing delays of each intermediate system, produce the transaction latency.
given anycast topology, one of the most important benefits of anycast is improved performance. Anycast solves a key challenge of traditional multinode infrastructures—the challenge of rapidly optimizing routing (i.e., performance via minimized transaction latency) in environments with highly variable or transient routing conditions.

Recall that a name server (NS) resource record is used to specify a DNS authoritative server. An NS record is eventually resolved to an individual IPv4 or IPv6 address. Domain name operators traditionally have specified multiple NS records to enhance client proximity and system resiliency and thereby minimize transaction latency. However, client resolver functions (or recursive name servers on their behalf) still need to learn which authoritative servers within a given NS record set produce the lowest transaction latency over time and then employ a localized algorithm to prefer those servers for the bulk of their queries while also continually seeking more optimal alternatives across other name servers in the NS set. This learning function is referred to as “server affinity” and, while implementation algorithms vary somewhat, it is common in most recursive name server implementations today.

In general, server affinity is desirable if the system is stable, but with the array of variables in IP-based networks, transaction latency of a given server is often temporal, and affinity of a given server may actually result in suboptimal server selection. The BIND server affinity algorithm, which is used in many name servers today, adapts reasonably well over time, but even it does not adapt rapidly enough to accommodate short-lived conditions induced by transient routing or other such variables in the network.

Anycast addresses this shortcoming. With anycast, a single NS record’s corresponding IP service address is made available simultaneously at multiple locations in the network. This approach allows domain name operators to optimize authoritative server locations for client proximity without having to specify large numbers of NS records and without requiring recursive name servers to learn which authoritative servers offer the lowest transaction latency and then guess about the current availability and transaction latency of other servers in the set. These capabilities help reduce query latency, making anycast a valuable tool for high-performance DNS resolution.

**Name Server (NS) Resource Records**

NS resource records specify which name servers within a zone are authoritative and should be queried during the resolution process. Each parent zone contains a database of NS resource records for its zone.

**Good for Some, but Not All, Use Cases**

Although most DNS services employ anycast because it significantly reduces query resolution latency, anomalies or conflicts can occur that cause resolution outages or prevent queries from resolving. The number of anycast-related outages is relatively small, but some outages are long in duration (approximately 30 percent of all transient routing conditions last more than 100 seconds¹). For this reason, anycast alone is seldom feasible in scenarios that require extremely high system availability and query resolution success.

When considering anycast use cases, it is important to recognize that IP routers forward packets on a hop-by-hop basis and make autonomous forwarding decisions. In addition, routing on the Internet is both dynamic and topologically localized. These characteristics can create resolution errors in long-lived transactions. For example, if TCP were used during a transaction and a routing change occurred that directed a client to a

---

When to Use Anycast

Anycast is best for short-lived, connectionless transactions where performance is the priority. A pure anycast solution may not be ideal for scenarios that require high availability or exhibit long-lived sessions.

Best to Divide Routing Among Multiple Nodes or Locations

Clearly, increasing the number of anycast nodes affects the number of queries being directed to the closest instance. At the same time, this approach destabilizes resolution services overall by increasing the number of server switches and unanswered queries, and by increasing the probability that a component at the systemic level will exhibit aberrant behavior that may result in resolution failure.

As mentioned earlier, when a query is unanswered within some short timeout window (usually one second or less), recursive name servers transmit one or more queries to other name servers in the zone's NS\ resource record set to attempt resolution elsewhere. If all the NS records are anycast to the same locations when routing system instability or resolution failures occur, all the congruent name servers behind the impacted network path are likely impacted. This condition prolongs the resolver's failover to another set of servers or results in a completely failed resolution process.

For this reason, when two or more anycasted authoritative name servers are employed for a common zone, Verisign recommends dividing the server routing among multiple, separate nodes. In other words, the servers should not share a common network footprint, and all other shared dependencies should be minimized as much as possible. (Similarly, unicasted name servers should be as physically and logically diverse as possible, so as to minimize shared dependencies and resulting failures in an NS record set for a given zone.)

Cautions aside, anycast enables organizations to expand capacity on a given IP service address. With this additional capacity, organizations can minimize bootstrapping functions and configuration for clients, optimize routing for client proximity, and distribute and topologically localize both legitimate query loads and attack loads. In addition, organizations gain massive scalability via the inherent caching and distributed database architecture on the resolution side of DNS.

Table 2 describes anycast benefits and challenges in further detail.

### USING HYBRID ROUTING TO OPTIMIZE RESOLUTION PERFORMANCE AND RELIABILITY

Although many domain operators choose anycast routing because it accelerates DNS resolution by minimizing transaction latency, the use of anycast alone implies a tradeoff between performance and availability.

Many domain operators would be better served by a hybrid solution, where some smaller number of name servers within a zone is anycasted, while the remaining servers are unicasted. This approach helps minimize transactional latency while optimizing the availability of the relevant zones.

Identifying the intersecting “sweet spot” in hybrid deployments, where the number of unicast and anycast
While resolution is core to DNS service, it is only one component of a complete DNS solution. Other vital functions include reporting, managing and auditing changes to zone records, and rapidly propagating domain name changes out to the DNS infrastructure. Verisign has the proven expertise, processes, and global infrastructure to provide a highly resilient, comprehensive solution that addresses the critical needs of organizations operating at all levels of the Internet ecosystem.

Verisign Managed DNS is a cloud-based DNS hosting service that delivers 100 percent DNS resolution availability while optimizing performance. The Managed DNS service helps organizations guarantee reliable, accurate, and timely resolution of DNS queries by leveraging a worldwide, securely managed DNS infrastructure and enabling a unique hybrid of unicast and anycast routing configurations.

Verisign’s fully redundant, globally

### Table 2 – Anycast Benefits and Challenges

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables organizations to expand footprint and capacity available on a given IP service address.</td>
<td>Occasionally succumbs to resolution anomalies or conflicts that impede resolution and compromise availability; occasionally introduces difficult-to-diagnose pockets of suboptimal routing when new servers use new paths to resolve an IP address.</td>
</tr>
<tr>
<td>Reduces latency and enhances performance by optimizing for client proximity to authoritative name servers.</td>
<td>Increases complexity of configuring zones, distributing zone updates, and maintaining near real-time zone coherency.</td>
</tr>
<tr>
<td>Helps balance, distribute, and localize query loads.</td>
<td>Potentially interferes with performance monitoring. IP-based monitoring is topologically dependent on the underlying routing system. Depending on the system's routing preferences, some monitoring queries may be directed to the wrong servers, simply because those servers respond more quickly than others in the zone.</td>
</tr>
<tr>
<td>Provides massive scalability via inherent caching processes and a distributed, decentralized resolution database architecture.</td>
<td>Impairs troubleshooting and problem diagnosis. Identifying a specific anycast instance or corresponding intermediate network elements that could be causing problems for a given set of clients is significantly more difficult.</td>
</tr>
<tr>
<td>Strengthens resistance to denial of service (DoS) and distributed denial of service (DDoS) attacks by increasing redundancy and distributing resolution activities across more geographically disperse locations.</td>
<td>Increases difficulty of detecting security threats. Detecting rogue routing system elements (e.g., route hijacks), static routed instances (only visible in the data path), and Byzantine failures is more difficult when systems become more complex, and a single persistent and more deterministic data path to the service address no longer exists.</td>
</tr>
</tbody>
</table>
Table 3 – Guidelines for Optimizing Resolution

<table>
<thead>
<tr>
<th>Goal</th>
<th>Verisign Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximize resolution and availability</td>
<td>Use anycasted name servers plus one or more unicasted servers. When placing unicasted servers, consider the demographics of querying recursive name servers; that is, place unicasted servers close to your data center, your customers, or both.</td>
</tr>
<tr>
<td>Maximize performance and minimize latency</td>
<td>Use only anycasted name servers.</td>
</tr>
<tr>
<td>Minimize failures in anycast environments</td>
<td>Ensure that the name servers specified for a domain are unique anycast announcements. Do not allow all specified name servers to go to all available nodes. In addition, ensure that authoritative servers for a zone do not share a common footprint; otherwise, if one node goes down, all name servers may fail. Alternatively, utilize two discrete unicast servers.</td>
</tr>
</tbody>
</table>

Figure 1 – Verisign DNS Resolution Sites

proprietary high-performance name resolution server, and is monitored around the clock. In addition, each site is based on redundant server architecture and uses a complete set of diverse hardware components and supporting network infrastructure to minimize shared dependencies and eliminate single points of failure. With Verisign’s massively scalable infrastructure and industry-leading...
service levels, organizations can confidently alleviate the financial burden and operational complexities associated with deploying and managing DNS infrastructure in house. At the same time, they gain the flexibility to tailor name servers for maximum performance, maximum reliability, or balanced performance and reliability. This capability to create a hybrid solution that meets each organization’s business needs is a key differentiator of the Verisign solution.

ABOUT VERISIGN
Verisign is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, our services allow public and private sector organizations, along with consumers all over the world, to engage in trusted communications and commerce.

LEARN MORE
For more information about hybrid anycast and unicast routing solutions and Verisign Managed DNS, please contact us by phone at 1-866-200-1979 or 1-703-376-6905, send an email to learnmore@Verisign.com, or visit VerisignInc.com.