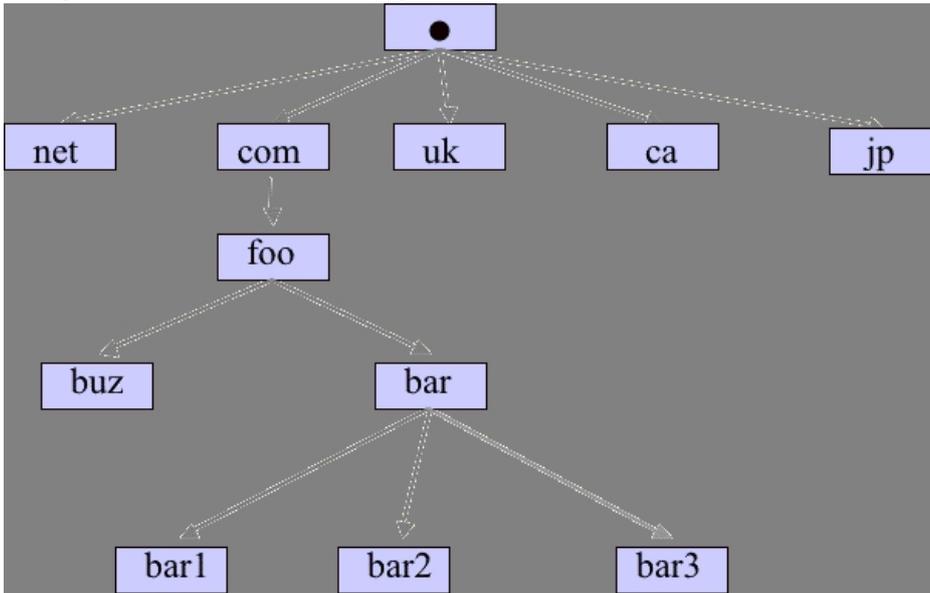# ⬜ Impact of misconfigurations

During the past twenty years the Domain Name System (DNS) has sustained phenomenal growth while maintaining satisfactory performance. However, the original design focused mainly on system robustness against physical failures, and neglected the impact of operational errors such as misconfigurations. Our recent measurement effort revealed three specific types of misconfigurations in DNS today: lame delegation, diminished server redundancy, and cyclic zone dependency. Zones with configuration errors suffer from reduced availability and increased query delays up to an order of magnitude. Furthermore, while the original DNS design assumed that redundant DNS servers fail independently, our measurements show that operational choices made at individual zones can severely affect the availability of other zones. We found that, left unchecked, DNS configuration errors are widespread, with lame delegation affecting 15% of the DNS zones, diminished server redundancy being even more prevalent, and cyclic dependency appearing in 2% of the zones. We also noted that the degrees of misconfiguration vary from zone to zone, with most popular zones having the lowest percentage of errors. Our results indicate that DNS, as well as any other truly robust large-scale system, must include systematic checking mechanisms to cope with operational errors.

DNS vs. DHT-based naming systems

The current Domain Name System (DNS) follows a hierarchical tree structure. Several recent efforts proposed to re-implement DNS as a peer-to-peer network with a flat structure that uses Distributed Hash Tables (DHT) to improve the system availability. As part of our work we compared the performance and availability of these two designs, enabled by caching and redundancy in both cases. We showed that the caching and redundancy mechanisms in each design are closely bound to its system structure. We further demonstrated that each of the two system structures provides unique advantages over the other, while each has its own shortcomings. Using analysis and trace-driven simulations, we show that hierarchical structure

enables high performance caching and that DHT structures provide high degree of robustness against targeted attacks. We further showed that the current DNS design offers engineering flexibilities which have been utilized to optimize system performance under typical Internet failures and traffic loads, and which can be further extended to overcome DNS weaknesses against the aforementioned attacks.

Anycast
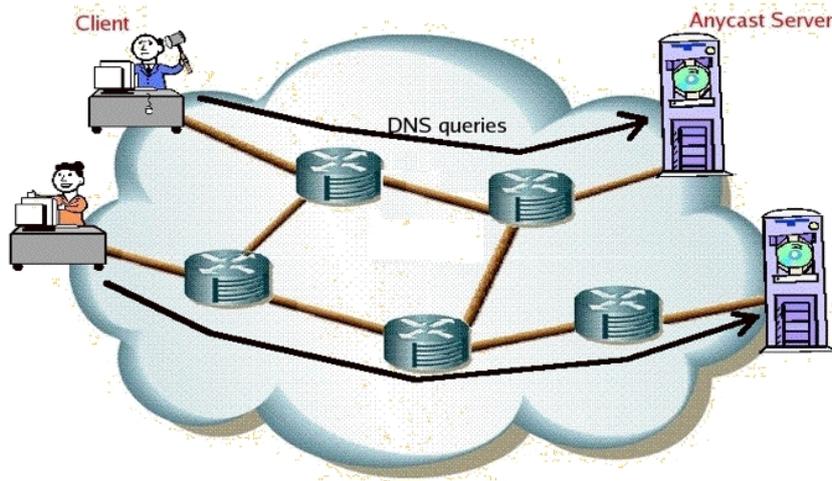
Given the fact that *anycast* is widely used by DNS, it is important to understand how well it performs in terms of reduced query latency and reduced outage times. To find the answer to these questions, we studied four top-level DNS servers to evaluate how anycast improves DNS service and compare different anycast configurations. Increased availability is one of the supposed advantages of anycast and we found that indeed the number of observed outages was smaller for anycast, suggesting that it provides a mostly stable service. On the other hand, outages can last up to multiple minutes, mainly due to slow BGP convergence. We also found that anycast indeed reduces query latency. Furthermore, depending on the anycast configuration used, 37% to 80% of the queries are directed to the closest anycast instance. Our measurements revealed an inherent trade-off between increasing the percentage of queries answered by the closest server and the stability of the DNS zone, measured by the number of query failures and server switches.

Project Members

- Andreas Terzis , JHU
- Sandeep Sarat , JHU
- Vasilis Pappas, IBM Research
- Lixia Zhang, UCLA
- Dan Massey, Colorado State University

Publications

- S. Sarat, V. Pappas, A. Terzis, **On the Use of Anycast in DNS**, Appeared in the Proceedings of ICCCN 2006.
[PDF](#)

- V. Pappas, D. Massey, A. Terzis, L. Zhang, **A Comparative Study of Hierarchical and DHT Based Naming Systems**   . Appeared in the Proceedings of INFOCOM 2006.
[PDF](#)

- V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, L. Zhang, **Impact of Configuration Errors on DNS Robustness**   .Presented at ACM SIGCOMM'04, Aug. 2004.
[PDF](#)