Asia Pacific Top Level Domain Association – www.aptld.org

APTLD Background Paper

Anycast - Robust DNS Services

APTLD is the Association of Top Level Domain operators in the Asia Pacific region

APTLD has produced this report on Anycasting as an aid to our members and other TLD operators. APTLD has a vision that all Top Level Domain operators in the Asia Pacific region will run secure, stable, resilient and successful operations to serve their respective communities. Our mission is to achieve our vision through Information, Education and Advocacy. This report helps in our mission to achieve our vision.

Contents

What is Anycast?

Anycast is a network routing methodology that announces the same address from many servers, often in diverse physical locations. It is used by TLD operators to improve the responsiveness and to provide greater redundancy and resiliency of their service. It is particularly useful in the event of a failure or an attack.

The nature of most DNS software is such that an end user's resolver will seek the 'fastest' authoritative server (as measured by round trip time) to answer its query, and if that server does not respond, will seek other servers farther (longer in time) away until its query is answered.

Anycast enhances this nature by leveraging the routing system to allow the queries sent out by the resolver to be directed to the nearest server in terms of network topology.

Perhaps more importantly, Anycast improves total system resilience. Administrators can "turn down" an Anycast instance by simply having that instance cease announcing its IP address to the routing system. When the route to the instance being turned down goes away, queries will be sent to the other instances that are still announcing their address.

Since Anycast localizes traffic it can help protect against some attacks.

DNS is inherently resilient. An Anycast solution can be used to not only improve on the resiliency of the service, but also increase its performance. However, careful consideration needs to be undertaken when designing the deployment of an Anycast solution.

Why is Anycast important?

Top Level Domain operators play an essential part in the Internet and its Domain Name System. The TLD operator keeps a list of the name servers where Second Level Domains can be found. While the queries TLD name

servers receive and their answers are relatively small, they are very frequent. It is good practice, in fact it is a requirement imposed by IANA, to have multiple locations so that in the event of a problem, either a failure or a malicious attack, queries will still be answered.

Anycast provides a methodology that allows a diverse set of servers that use the same IP address to answer queries – and the greater diversity the greater the value of the service. Diversity can be measured in geographic diversity, but also network diversity, hardware brand diversity, software diversity, and local infrastructure diversity – including power.

While some TLD operators own and operate their own set of diverse servers, or have bilateral relations with other TLD operators, there are Anycast service providers whose core business is providing robust and diverse infrastructure for the hosting of TLD DNS services.

Why you might NOT want to use Anycast

While Anycast absolutely increases the ability to respond to a DNS query it does so at the cost of increased complexity. Furthermore, in traditional (Unicast) DNS, the selection of which server to query lies in the resolver, i.e. in the "DNS layer", while in Anycast DNS this selection moves down into the routing layer. Typically it will be more difficult to analyse and debug the Anycast behavior, due to this dependency on the underlying routing layer for server selection.

How can Anycast be deployed?

There are a wide variety of models for Anycast deployment – each with their own advantages and disadvantages:

- **Owner Operated**: In this model the TLD will own and operate the Anycast servers at different locations. This gives the TLD the most control and, for comparable levels of service, the highest cost.
- **Bi-Lateral:** In this model, TLD operators will form bi-lateral agreements with other TLD operators who will provide the service on a reciprocal basis. These are traditionally at zero or low cost but provide limited diversity and are generally provided on a 'Best Endevour' basis.
- **Multi-Lateral:** In this model, a group of TLD operators will form reciprocal agreements with other TLD operators. These are traditionally at zero or low cost but the service is generally provided on a 'Best Endeavour' basis.
- **Not-For-Profit:** In this model, a not-for-profit organisation that exists to serve the local, regional or global Internet community will offer an Anycast service. These can be at zero cost or there may be a cost recovery fee applied.
- **For Profit Operators:** In this model, the Anycast provider operates on a commercial basis. This model will generally have a higher cost. Some For Profit Operators will provide an Anycast service for smaller TLD at zero or low cost as a service to the community and to build their name base – which then provides a market differentiator when they pursue commercial clients – which could include very large registrants who are looking for global reach and robust and resilient services. Think CNN or Amazon as examples.

It is quite common for TLD operators to make use of two or more Anycast service providers.

It is very important to have a strong and clear Service Level Agreement (SLA) with any other entities that are part of providing the Anycast service. The SLA should include details about minimum number of operational sites, response time for problems, access to stats and monitoring data, etc., i.e., while "best endeavour" at "low cost" may seem inexpensive it has major drawbacks when there are serious problems.

Features to consider when choosing an Anycast service provider

Relevant features of Anycast service providers include:

- **Cost**: The TLD operator will need to consider cost. There are a number of organisations that offer TLD operators Anycast service at no cost. Others charge a fee. And the fee could be a fixed fee, a per name fee, or a band of number of names.
- **Diverse Platforms** – hardware, software, and infrastructure. The hardware, operating system, name server software, and infrastructure systems such as routers, switches, etc., used should be diverse as well, just in case there's a system problem with any of them.
- **DNSSEC Support**: The service should also support DNSSEC, just as the TLD should.
- **Geographic Diversity**: Servers should be in different physical places – and the greater number of places and the greater diversity of the places the better. TLD operators should seek particular presence in those places around the world where most of their queries come from. *If you were running an internationalized (IDN) TLD in Chinese characters, one would expect that most of your traffic would come from Chinese speaking communities so you would seek geographic diversity within the Chinese speaking regions of the world.*

- **IPv6 support**: The service should support both IPv4 and IPv6, just as the TLD should.
- **Monitoring and Reporting –** the Anycast service provider should provide 24/7 monitoring and response services and the reporting should be timely and appropriate to the TLD's needs.
- **Network Diversity**: The Internet is a network of networks. There are some network operators with wide geographic reach. Putting servers on multiple nodes of the same network provider does not mitigate against the risk of a network failure (technical or commercial), so Anycast services should be provided on multiple physical networks under different ownership.
- **Proximity of Major Recursive Servers –** Some Anycast providers also host, or maintain server clusters adjacent to or with the recursive servers of major ISPs. Having your TLD name servers within or adjacent to large ISPs can improve end-user performance.
- **Resilient Infrastructure –** The infrastructure used by the Anycast service provider should be strong and resilient. The fewer the number of different sites, the greater the need for redundancy within each site. This may include multiple sources of electricity, UPS and backup generators, and transit services from multiple local network suppliers. The buildings should be secure with limited access. The more Anycast nodes, the more tolerable 'weaker' infrastructure would be at each node.
- **Secure Channels of Access**: It will be beneficial if the TLD has a secure channel (VPN) to access the Anycast sites, not just for Zone Transfers, but to also access the server and analyse its performance.
- **Service Level Agreement:** The terms of the contract, technical requirements and guarantees and remedies for poor performance should be specified in the contract.

Who can provide Anycast Services?

While the following providers of Anycast services have been identified by APTLD, **APTLD makes no warranty of their services nor does APTLD endorse them as service providers.** Their inclusion on this list is because they answered a call by APTLD to find Anycast service providers that would be interested in providing a service to ccTLDs.

Afilias	rlaplante@afilias.info
CommunityDNS	Paul.Kane@CDNS.net
DENIC	dbs@denic.de
Discovery DNS (ARI Registry Services).	sebastien.ducos@ariservices.com
Hostmaster	dk@hostmaster.ua
IPCom GmbH	monika.pink-rank@nic.at
Netnod	kurtis@netnod.se
Neustar	Fernando.Espana@neustar.biz
PCH	woody@pch.net
Technical center of the Internet (TCI)	o.baskakova@cctld.ru
Verisign	jseo@verisign.com