

DNS

DNS Infrastructure

NYCMesh maintains an internal DNS with the "fake" top-level domain (TLD) of `.mesh` (dot mesh). Through this, services can be hosted, internal sites, etc. Use **10.10.10.10** for your DNS server.

DNS configuration

The DNS is hosted using standard DNS zones which are made available through the Knot Resolver and Knot DNS Server.

The zone and scripts are made available via git. Once the master branch is updated, the DNS servers will periodically update and refresh their configuration.

Git Repo: github.com/nycmeshnet/nycmesh-dns

Git Repo: NYCMesh in-mesh git (does not exist yet)

Anycast DNS and IPs

Anycast

The DNS system is available through a "trick" called Anycast. Anycast is the number one way DNS is provided on the main public internet. With anycast, many DNS servers all present the same virtual IP. They announce this IP in the routing table (mesh routing table, BGP or other protocol). With this, the clients believe they all have a very short route to the same network, but in fact it is a copy of the same service running many times with the same configuration. Any of the services may answer the request equally well. Reply packets are sent via the normal means.

IPs

10.10.10.10 - Resolving DNS endpoint for the mesh (**Use this one**)

10.10.10.11 - Authoritative endpoint for dot-mesh TLD.

199.167.59.10 - Public DNS Resolver for anyone in the world. No Logs, No filtering.

The reason for two endpoints rather than one is to enable resolving the dot-mesh TLD separately. In-fact, the caching resolver forwards to the dot-mesh TLD server for dot-mesh addresses. This also allows more than one node to host a resolver, or, a dot-mesh DNS server, or both.

Top Level Domains

- `.mesh` - Internal dot-mesh domain for NYC Mesh.
- `.mesh.nycmesh.net` - Public version of the same domain. Equivalent of `.mesh`. Available on the entire internet

Running a DNS Server

This is a Work in progress

Today there is a DNS server run at Supernode 1 as a VM. More are planned. It would be nice if at least every supernode ran a DNS clone.

In the future it is expected that anyone who wants to run one can do so using a Docker container etc.

To get a jump-start on this, check out the Git repo and take a look at the README. It's an ever-changing process.

Revision #2

Created 9 December 2023 04:39:48 by Willard Nilges

Updated 16 December 2023 03:07:42 by Andy