Everything you know about DNS is wrong

But it's not your fault.

Let’s start by addressing that title.

- The interim title “DNS - It's always DNS”, saved you from a dry talk about what DNS that probably would have used the same analogies that are a problem.
- DNS is the backbone of the internet. And in helping people debug issues that involve DNS, one of the major issues is that there expectations don’t match how DNS is being used.
- DNS is a tool that has been around since 1984, (BIND in particular) and as one of the early tools of the internet it is used to solve lots of problems that it wasn’t conceived to handle.

DNS is not a phone book for humans.

- fiddle-calliope-crh8.squarespace.com is the DNS name for the website of a business I frequent. The staff do not know this URL. They think it is weird that I do.
- URL shorteners like bit.ly have URLs that no human will remember. And they return full URLs with hostnames not ips.
- QR codes don't embed IPs instead of hostnames even though that can be shorter.
- Your browser will fight you when trying to enter a URL if you have previously put in something similar

There is no such thing as a reverse lookup

- Often DNS is presented as a name, ip duple with forward lookups being those starting with the name and reverse starting with the ip. A name pointing to an ip and an ip pointing at a name have nothing to do with each other.
- Multiple names can resolve to a single IP address.
- The authoritative records for the name and the ip can be on different servers controlled by different organizations.
- If you control resolution for a record you can have it point anywhere you want.

At the beginning of a DNS query you talk to one of the 13 root servers

- typical endpoints will know about the root servers but will never query them.
- A manual network configuration will normally include a DNS server, this is never one of the root DNS servers
- If you can't get to your DNS server your computer will insist that you aren't connected to the internet without even trying to talk to the root servers.
- Private IP space is usable for big organizations because they can be between you and the roots and tell you about the ips no one is authoritative for.

So what is DNS really used for?

- Abstracting resources to make upgrades hitless. And allow other dynamic infrastructure
- As a load balancer that doesn't have to be a single point of failure.
- For service discovery
- For virtualization of resources.
- Application authentication
- Spam prevention.

What about IP lookups.

- An IP lookup is just like a hostname lookup, but in a special domain. in-addr.arpa.
- The IP address 128.8.120.19 will be looked up as 19.120.8.120.in-addr.arpa. ipv6.arpa for ipv6
- If you use subnetting so that a local network is bigger or smaller than 256 addresses the IPs will still be in divided by the byte boundaries in the IP. So for big subnets to IPs might be in different domains, and for small subnets you might have address from many networks in one domain. These are not IP lookups that are savvy to things IP, they are domain name lookups

So what happens when you make a query?

- You make a list of names to check for based on search domains. Which it tries one at a time.
- You check your local hosts file
- You try the DNS servers you have defined one at a time
- If you get through to a server it:
  - Checks to see if it’s got any locally defined records relevant to the lookup
  - Checks to see if it’s got any records relevant to the lookup cached
  - Starts with the lookup tree where the previous two steps left off, maybe starting all the way at the root
  - Applies any cyber squatting rules it has to serve you ads.

- After painfully timing out through all of that you give up

Now for the nuts & Bolts

The basics - the records

- A DNS record looks like:

```
NAME TTL CLASS TYPE DATA

faculty    3600  IN   CNAME  umiacswww-vip.umiacs.umd.edu.
```

- The name is the record you are looking up.
- The TTL is how long this record may be cached for in seconds. If not specified it uses the next level up
- The Class is “IN”, this is optional. This is a feature that wasn’t ever really used (maybe some day)
- The type is the type of record, we’ll say more on the next slide
- The data is type dependent but it going to be the data you were trying to get.
- Most records exist in the context of an ORIGIN statement. This record was under the origin umiacs.umd.edu.

The basics - the record types

- A - These records hold IP addresses like 128.8.120.19
- AAAA - These records hold IPv6 addresses
- CNAME - These are like aliases and have another hostname
- MX - this provides the name of the mail handlers for the record
- TXT - This a generic string. There can be many of these for one name
- NS - This is used to indicate the name server(s) to talk to for the name. These can be chained
- SOA - Tells you about the admins of the name, generally only domains will have these. ie umd.edu will have one but not www.umd.edu
- SRV - used for service discovery.
- PTR - Used for looking up IPS returns domains. IPv4 and IPv6 don't collide so only one type is needed for both.
- There are some less commonly used record types that we won't discuss.

The basics - looking up

- host - simplest quasi-deprecated command. Uses search domains, guesses you're looking for A,MX or PTR based on query
- nslookup - also quasi-deprecated. Uses search domains, guesses A or PTR. Provides info about the lookup
- dig - current?. No search domains. Assumes A. Provides more info about the lookup. -t will let you specify the type
- ping - not officially a DNS lookup command but will resolve through the system, and get entries from /etc/hosts

Abstracting resources for dynamic infrastructure

- If you’re going to be changing out a piece of infrastructure you use a name as the magic string. Often a CNAME
- Before the change lower the TTL on the record.
- Change the record
- Wait the length of the TTL then turn off the old one.
- If the 2 versions can co-exist this can be hitless.

As a load balancer without a single point of failure.

- A name can have multiple NS records and these work pretty well for redundancy.
- When you lookup the server you get the ip that is under the least load.
- Don’t have a high TTL.
- Since it’s only the DNS resolution that goes through the load balancer(s) they don’t have to be as capable as the whole cluster combined

Service discovery

- MX and SRV records are used for service discovery
- MX is for mail, SRV is for everything else
- SRV records will generally be _SERVICE._PROTOCOL.DOMAIN
- _ipp._tcp.umiacs.UMD.EDU.
- Leading _ names are the “hidden” names.
- Can have multiple of these and they use PTR that resolve to SRV
- If needed can use TXT for additional arguments

Virtualization of resources.

- This is mostly on the web but potentially any protocol where what you requested is part of the request.
- A web server might have dozens of virtual hosts, and it determines how to resolve based on the name of the host in the URL that got you there.
- This is why editing /etc/hosts is crucial for testing webservers

Application authentication

- This is in TXT records.
- Applications will let you get their data about you if you put the string they gave you in a TXT record.

Spam prevention

- This uses TXT records.
- SPF uses this to authorize hosts to relay for your domain.
- DKIM uses this to provide public keys for signature verification

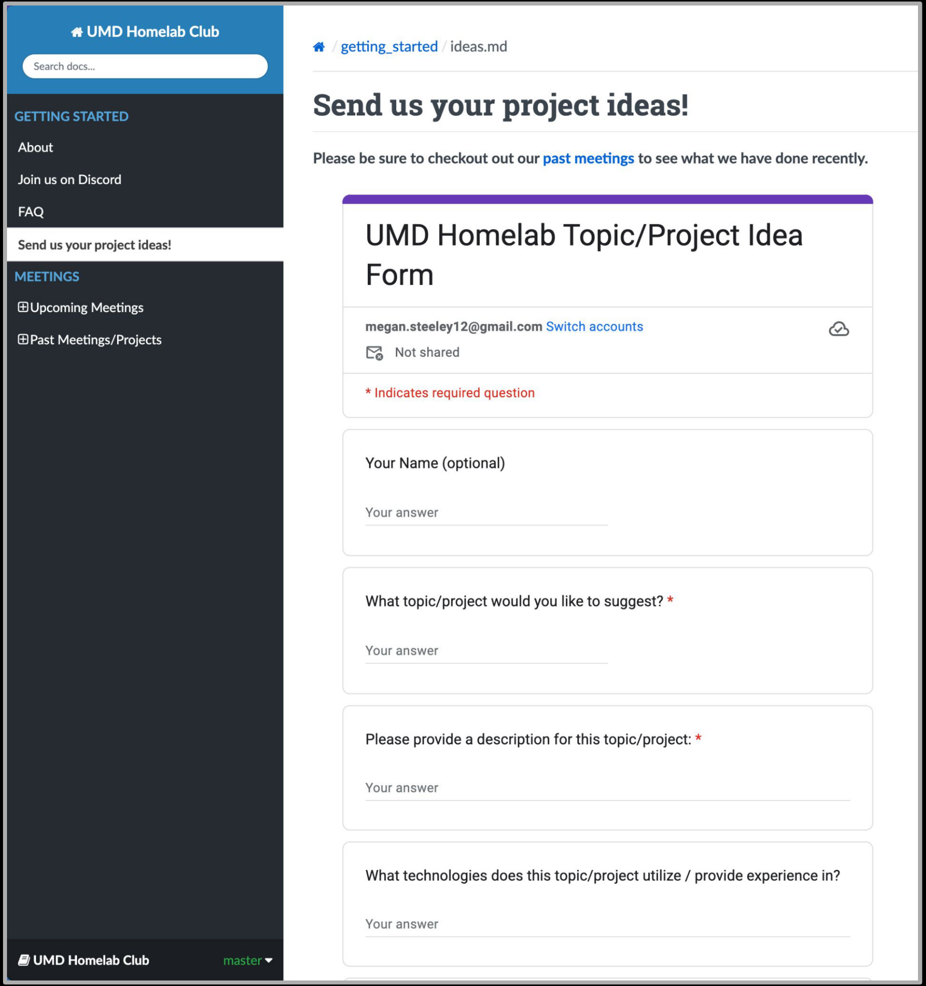
The tree hierarchy dance.

- You start with . The end of every FQDN (fully qualified domain name).
- There are 13 servers that serve this they are called the root servers, they are a big deal. UMD has one.
- Then you ask them for the NS record for the next down.
- You ask that for the same NS record stopping when you get a self reference
- Then you ask it about the next down. When you run out of NS records you ask for the other type.

There is a new project idea form

Ideas from this form will be used for future polls/votes

https://suddenlysixam.club/getting_started/ideas.html



Send us your project ideas!

Please be sure to checkout out our past meetings to see what we have done recently.

UMD Homelab Topic/Project Idea Form

megan.steeley12@gmail.com Switch accounts

Not shared

* Indicates required question

Your Name (optional)

Your answer

What topic/project would you like to suggest? *

Your answer

Please provide a description for this topic/project: *

Your answer

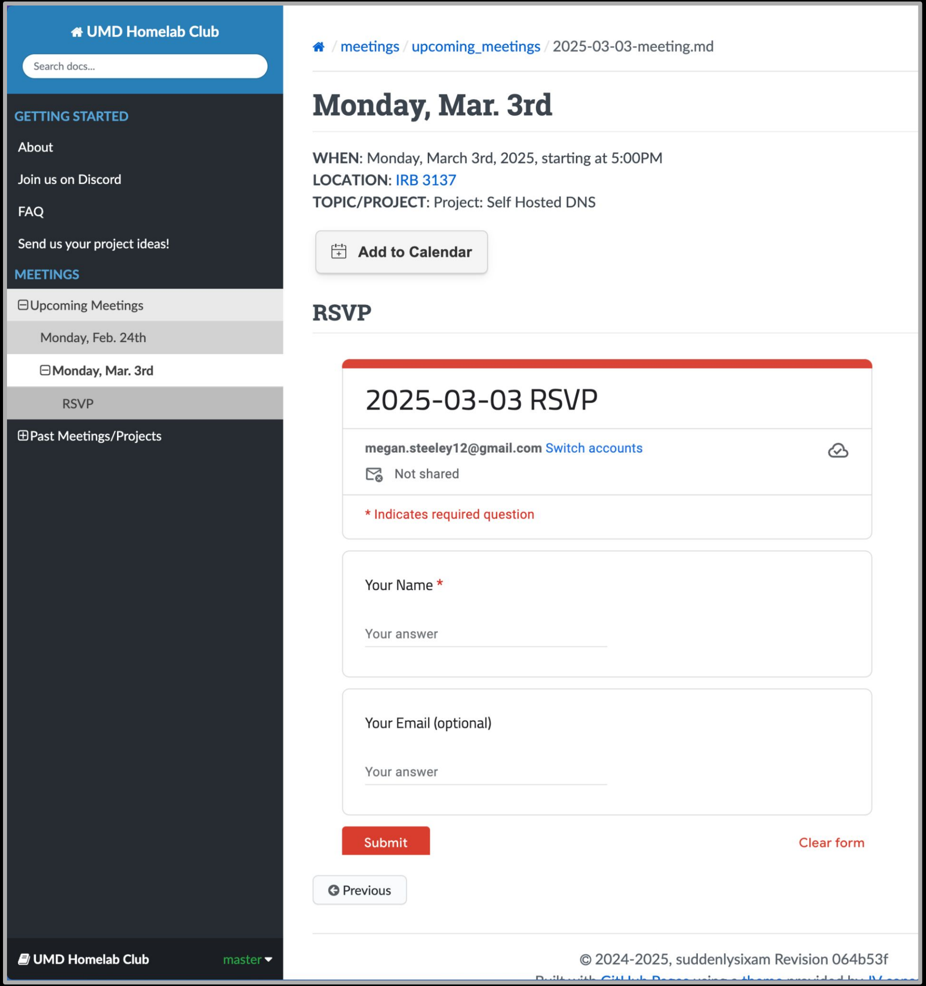
What technologies does this topic/project utilize / provide experience in?

Your answer

Next week is a demo

RSVP's are required (either in the Discord or through the form on the website)

https://suddenlysixam.club/meetings/upcoming_meetings/2025-03-03-meeting.html



Monday, Mar. 3rd

WHEN: Monday, March 3rd, 2025, starting at 5:00PM
LOCATION: IRB 3137
TOPIC/PROJECT: Project: Self Hosted DNS

RSVP

2025-03-03 RSVP

megan.steeley12@gmail.com Switch accounts
Not shared

* Indicates required question

Your Name *
Your answer

Your Email (optional)
Your answer

© 2024-2025, suddenlysixam Revision 064b53f

Thank you!

Don't forget to join the Discord!

https://suddenlysixam.club/discord