ECE 435 – Network Engineering
Lecture 11

Vince Weaver

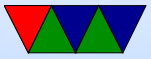
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

18 February 2026

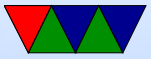
Announcements

- HW#3 was due (sorry for making it due President's Day)
- HW#4 will be Posted
  Using tools to access DNS info, let me know if you have trouble.
- Working on getting outstanding homeworks graded



Domain Name System (DNS)

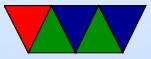
- Used to map hostnames to IP addresses
- Hierarchical distributed database
- Why do we need it?
  - Can you remember numbers? Send e-mails to vince@192.168.8.1?
  - What if server moves?
- RFC 1034/1035 (1987), supersedes RFC 882/883 (1983)



DNS Importance

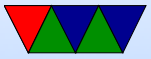
- If there's a network problem, it's "always DNS" (or maybe BGP)
- One example: big Amazon AWS outage in October 2025

  `https://www.theregister.com/2025/10/23/amazon_outage_postmortem/`



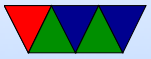
Ancient History

- In early days NIC.arpa had a "HOSTS.TXT" file you downloaded occasionally with all known machines. Didn't really scale.
- Trivia, called SRI (stanford research) on phone to get Elizabeth "Jake" Feinler during business hours and she'd manually add you to list.
- /etc/hosts is a relic of this, usually checked first



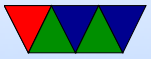
IP Address Lookup on Linux

- Traditionally this configured via `/etc/nsswitch.conf`
- Could specify multiple ways to search, with different priorities:
  - files (/etc/hosts)
  - dns
  - mdns (dns-like automatic resolving on local networks)
  - nis/ldap (local directory services)



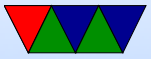
Domain Names

- Which ones can you name? .com/.org/.gov/.edu/.net/.mil
- Country codes (.us/.uk/.ie etc) (.io drama)
- Huge expansion in the last few years (.horse)
- Owner of a domain can subdivide, i.e. eece.maine.edu
- How do you buy them? Used to be fairly expensive and only for two years at a time from a single registrar. Not so much anymore.
- whois will show you info on who owns (less details than old days)



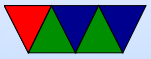
Name Rules

- Can have 127 levels, each 1-63 chars.
- Usually total name cannot exceed 253 chars.
- LDH (letters,digits,hyphens, cannot start with hyphen, not all numbers)
- Case-insensitive
- International names: "punycode". Trouble, why? Foreign letters that look like ASCII ones.
- punycode – snowman example `http://xn--n3h.net/`
- First commercial name 15 March 1985 symbolics.com



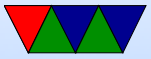
example.com set aside (why be careful with your example names?)

- Shortest? g.cn. Various one-letter domains (like x.org) but they were later reserved.
- Typosquatting, domain squatting, copyrighted names, etc.



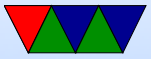
DNS Server

- Listens on port 53, usually UDP
  (Special case if $>$ 512 bytes: use TCP)
  Note the 512 byte UDP limit is a performance / fragmentation thing?
- A simple request might look something like:
  a bunch of flags specifying options
  `google.com type: A class: IN`
- A simpler response will restate the question then have the response: `google.com type: A class: IN: addr`



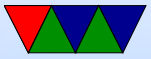
`1.2.3.4`

- Note it's a binary protocol, not chatty ascii text

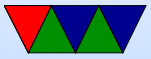


Zone Records

- 5-tuple, NAME TTL CLASS TYPE VALUE
  - TTL (how long to cache)
  - Class (usually IN for internet)
    Mostly reserved, with two obsolete networks chaos, hesiod
  - Type and RDATA (resource data)
  - Common types
    - SOA – start of authority (parameters) primary source, e-mail of admin, etc

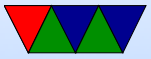


- A – IPv4 address of host (32bit int) `linux.deater.net 86400 IN A 1.2.3.4` can have multiple and be cycled through round-robin
- AAAA – IPv6
- MX – Mail exchange (can have multiple, can specify priority)
- NS – name sever (name server for this domain)
- CNAME – Canonical name, allows aliases (can have www.example.com point to example.com, then not have to update entry if example.com moves)
- PTR – alias for IP, for reverse lookup



`4.3.2.1.in-addr.arpa`

- HINFO – cpu and OS type (text) (uncommon)
- TXT – raw ASCII text
- SRV – new – sort of generic version of MX
- SPF – which machines can send e-mails (avoid spam)
- DKIM – keys for e-mail verification



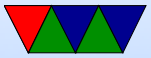
DNS Hacks

- Can you store other things in records? Text adventure? File transfer? Tunneling (iodine?)

- DNS filesystem, storing text files in other people's DNS resolver cache

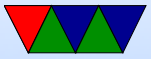
  `https://blog.benjojo.co.uk/post/dns-filesystem-true-cloud-storage-dnsfs`

- Why do this?
  - DNS often not blocked by firewalls
  - DNS often works even in face of captive portals



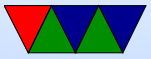
DNS Lookup – Client

- Basically: application calls a library (resolver) with the hostname.
  `gethostbyname()` HW#2
- Operating system / C library starts request (This example is how it goes on Linux)
  - First check `/etc/nsswitch.conf` to see what protocols to use. Might say to check local files (`/etc/hosts`) or local directory (NIS/LDAP) first
  - If DNS specified, looks up nameserver info



(`/etc/resolv.conf`)

- Sends DNS request via UDP to local nameserver



DNS Lookup – Nameserver

- Listens for request on UDP
- If happens to be official nameserver for this machine, get *authoritative response* (from responsible zone)
  the alternative is a cached response
- If local DNS server doesn't know about it, it has to ask up the chain.
- If totally not known, query "root" server. So if looking up weaver-lab.eece.maine.edu will ask root, which will direct to .edu DNS server