CSC 4350 – Computer Networks

Domain Name System (DNS)

September 17, 2024

Note

- Material in this lecture is heavily borrowed from Kurose & Ross' "Computer Networking: A Top Down Approach, 8th Edition"

DNS – Internet’s Directory Service

- Services Provided by DNS
- Overview of How DNS Works
  - Distributed, hierarchical database
  - DNS caching
- DNS Records and Messages
  - DNS Messages
  - Inserting Records into the DNS Database

Directory Service

- How can we be identified?
  - Driver's license number
  - SSN
  - Date of birth
  - One may be more appropriate than another, depending on context
- Identifier for a host – hostname
  - Mnemonic and appreciated by humans (www.google.com, www.apple.com)
  - Hostnames provide little, if any, information about the location within the internet of the host
  - Hosts identified via IP addresses
    - Consists of four bytes and has a rigid hierarchical structure
    - Each period separates numbers 0-255
    - Hierarchical – scan the address from left to right – more specific information obtained

Services Provided by DNS

- Reconcile preferences of names v. IP addresses – need a directory service that translates hostnames to IP addresses.
  - Main task of DNS
- DNS
  - Distributed database implemented in a hierarchy of DNS servers
  - An application-layer protocol that allows hosts to query the distributed database
  - Servers are often UNIX machines running Berkeley Internet Name Domain (BIND)

Example

- Browser running on some user’s host requests the URL www.someschool.edu/index.html
- In order to be able to send an HTTP request message to the web server www.someschool.edu, the user’s host must first obtain the IP address
- Steps
  - The same user machine runs the client side of the DNS application
  - The browser extracts the hostname www.someschool.edu from the URL and passes the hostname to the client side of the DNS application
  - The DNS client sends a query containing the hostname to a DNS server
  - The DNS client eventually receives a reply, which includes the IP address for the hostname
  - Once browser receives IP address from DNS, it can initiate a TCP connection to the HTTP server process located at port 80 at that address
- Potential delay for look-up

What Else Does DNS Do?

- Host aliasing
  - Host with a complicated hostname can have one or more alias names
    - Example: relay1.west-coast.enterprise.com
    - Could have two aliases: enterprise.com and www.enterprise.com
    - The relay1.west-cost… is said to be a canonical hostname
      - Alias hostnames are typically more mnemonic than canonical hostnames
    - DNS can be invoked to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host
- Mail server aliasing
  - If Bob has an account with Yahoo Mail, his address might be bob@yahoo.com
  - The hostname of the Yahoo mail server is more complicated and less mnemonic than yahoo.com
  - DNS can be invoked by a mail application to obtain canonical hostname for a supplied alias hostname as well as the IP address of the host
  - MX record permits company’s mail server and web server to have identical (aliased) hostnames
    - A company’s web server and mail server can both be called enterprise.com

What Else Does DNS Do?

- Load distribution
  - Buy sites are replicated over multiple servers, with each server running on a different end system and each having a different IP address
  - DNS database contains this set of IP addresses
  - When clients make a DNS query for a name mapped to a set of addresses, server responds with the entire set of IP addresses, but rotates the order of the addresses within each reply
  - DNS distributes the traffic among the replicated servers

How DNS Works

- Suppose some application running in a user's host needs to translate a hostname to an IP address
- Application will invoke the client side of DNS, specifying the hostname that needs to be translated
- DNS in the user's host then takes over, sending a query message into the network.
- All DNS query/reply messages are sent within UDP datagrams to port 53
- After a certain delay, the DNS in the user's host receives a DNS reply message that provides the desired mapping, then passed to the invoking application
- Might think of as a black box that implements the service is complex, consisting of a large number of DNS servers around the globe

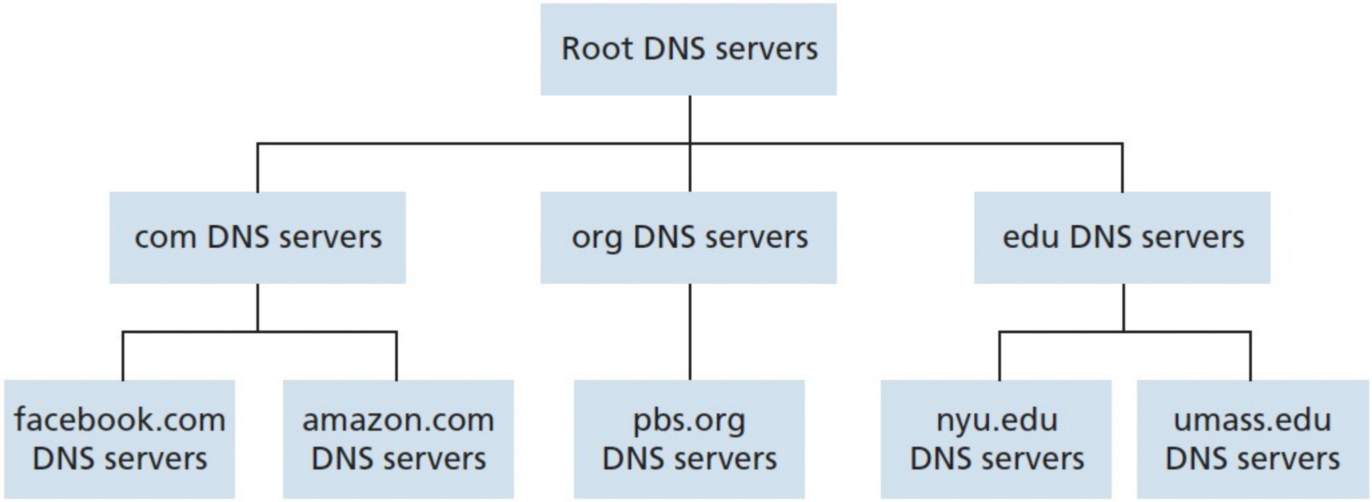
DNS and Centralized Design

- Clients direct all queries to the single DNS server
- DNS server responds directly to the querying clients
- Not appropriate for the growing number of hosts
- Problems
  - A single point of failure – if the DNS server crashes, so does the Internet
  - Traffic volume – a single server would have to handle all DNS queries for all of the HTTP requests/email messages generated by millions of hosts
  - Distant centralized database – a single DNS server cannot be “close to” all querying clients
    - If put in NYC, then all queries from Australia must travel to the other side of the globe, maybe even slow/congested links
  - Maintenance
    - Single DNS server would have to keep records for all internet hosts
    - Huge centralized database
    - Frequent updates for every new host

Distributed, Hierarchical Database

- Dealing with scale – DNS uses a large number of servers, organized in hierarchical fashion and distributed around the world
- No single DNS server has all the mappings for all of the hosts in the internet
- Mappings are distributed across the DNS servers
- First approximation – three classes of DNS servers
    - Root DNS servers
    - Top-level Domain DNS Servers (TLD)
    - Authoritative DNS servers
    - See next slide for possible placement/alignment

Figure 2.17 – Portion of the Hierarchy of DNS Servers



Example with Amazon

- DNS client wants to determine the IP address for www.amazon.com
- The client first contacts one of the root servers, which returns IP addresses for TLD servers for the top-level domain com
- Client contacts one of the TLD servers, which returns the IP address of an authoritative server for amazon.com
- Client contacts one of the authoritative servers for amazon.com, which returns the IP address of the hostname www.amazon.com

More on the Classes of DNS Servers

- Root DNS Servers
  - More than 1000 scattered all over the world
  - Copies of 13 different root servers, managed by 12 different organizations and coordinated through the Internet Assigned Numbers Authority (IANA)
  - Provide the IP addresses of the TLD servers
- TLD Servers
  - For each of the top-level domains - .com, .org, .net, .edu, .gov and country domains, there is a TLD server
  - Verisign Global Registry Services maintains the TLD servers for the com top-level domain
  - Educause maintains the TLD servers for the edu top-level domain
  - Etc.

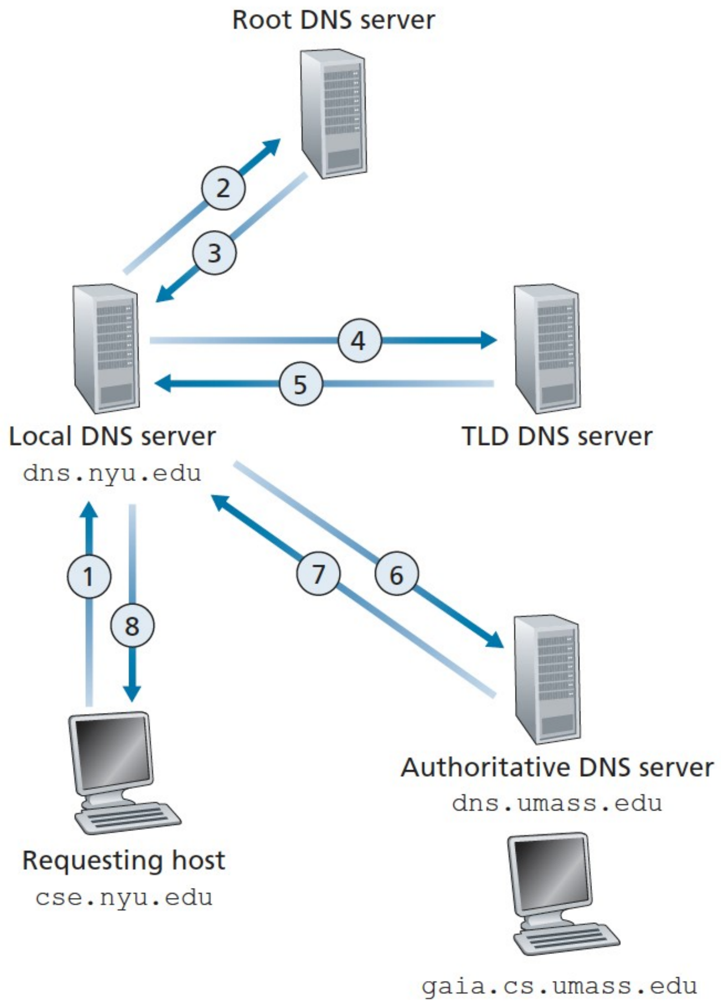
More on the Classes of DNS Servers

- Authoritative DNS Servers
  - Every organization with publicly accessible hosts on the internet must provide publicly accessible DNS records that map names to IP addresses
  - Organization can choose to implement its own authoritative DNS server
  - Alternative: organization pays to have these records stored in an authoritative DNS server of some service provider
  - Most companies/universities maintain their own primary/secondary authoritative DNS server
- Local DNS Server
  - Does not strictly belong to the hierarchy of servers, but part of DNS architecture
  - Each ISP has a local DNS server
  - When a host connects to an ISP, the ISP provides the host with the IP addresses of one or more of its local DNS servers
  - Host’s local DNS server is typically “close to” the host

Example – Trying to Get to gaia.cs.umass.edu

- Host cse.nyu.edu sends a DNS query message to its local DNS server, dns.nyu.edu
- Query message contains the hostname to be translated (gaia)
- Local DNS server forwards the query message to a root DNS server
  - Takes note of the edu suffix and returns to the local DNS several IP addresses for TLD servers responsible for edu
- Local DNS server resends query to one of the TLD servers
  - TLD server takes note of the umass.edu suffix and responds with the IP address of authoritative DNS server for Umass
- Local DNS server resends the query message directly to dns.umass.edu
  - Responds with the IP address of gaia.cs.umass.edu
- Use recursive, iterative queries – in theory, any query can be iterative or recursive
- Normal pattern: query from the requesting host to the local DNS server is recursive, remaining queries are iterative

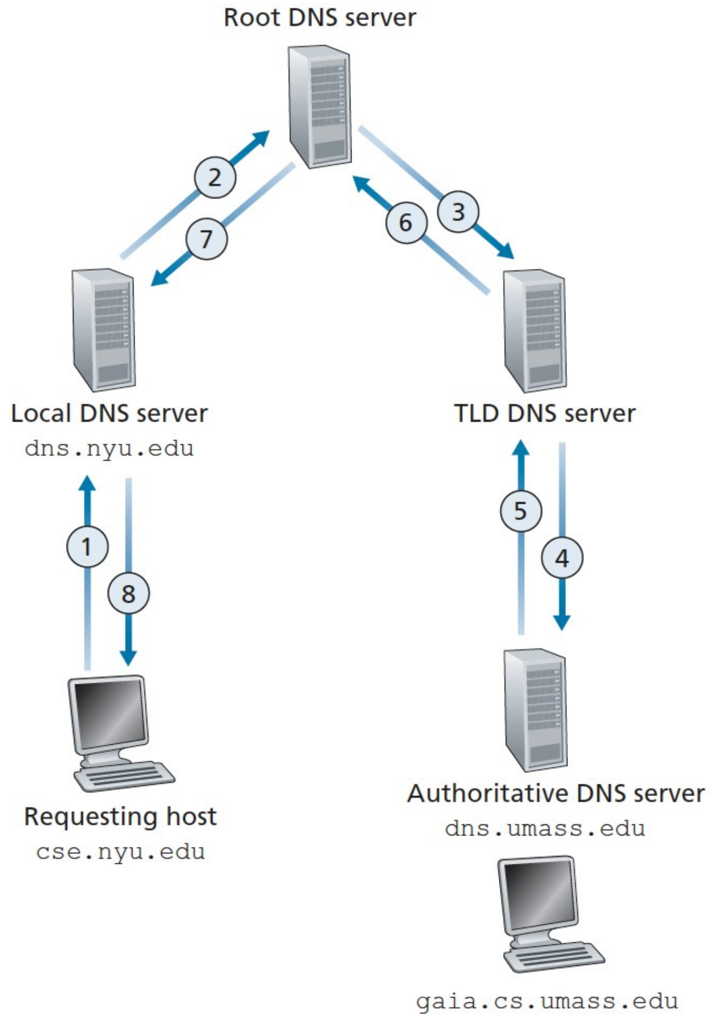
Figure 2.19 – Interaction of the Various DNS Servers



DNS Caching

- Used a bit to improve the delay performance and reduce the number of DNS messages coming from around the internet
- In a query chain, when a DNS server receives a DNS reply, it can cache the mapping in its local memory
- If hostname/IP address pair is cached in a DNS server and another query arrives to the DNS server for the same hostname, the DNS server can provide the desired IP address
- DNS servers discard cached information after a period of time

Figure 2.20 – Recursive Queries in DNS



DNS Records and Messages

- DNS servers that implement the DNS distributed database store resource records (RRs), including those that provide hostname-to-IP address mappings
- Each DNS reply message carries one or more resource records
- An RR – four-tuple that contains the following fields
  - Name
  - Value
  - Type
  - TTL – time to live of the resource record
  - Meaning of Name and Value depend on Type

Resource Records…

- If Type = A
  - Name is a hostname
  - Value is the IP address for the hostname
  - Example: (relay1.bar.foo.com, 145.37.93.126, A) is a type-A record
- If Type = NS
  - Name is a domain
  - Value is the hostname of an authoritative DNS server that knows how to obtain the IP addresses for hosts in the domain
  - Example: (foo.com, dns.foo.com, NS) is a type NS record

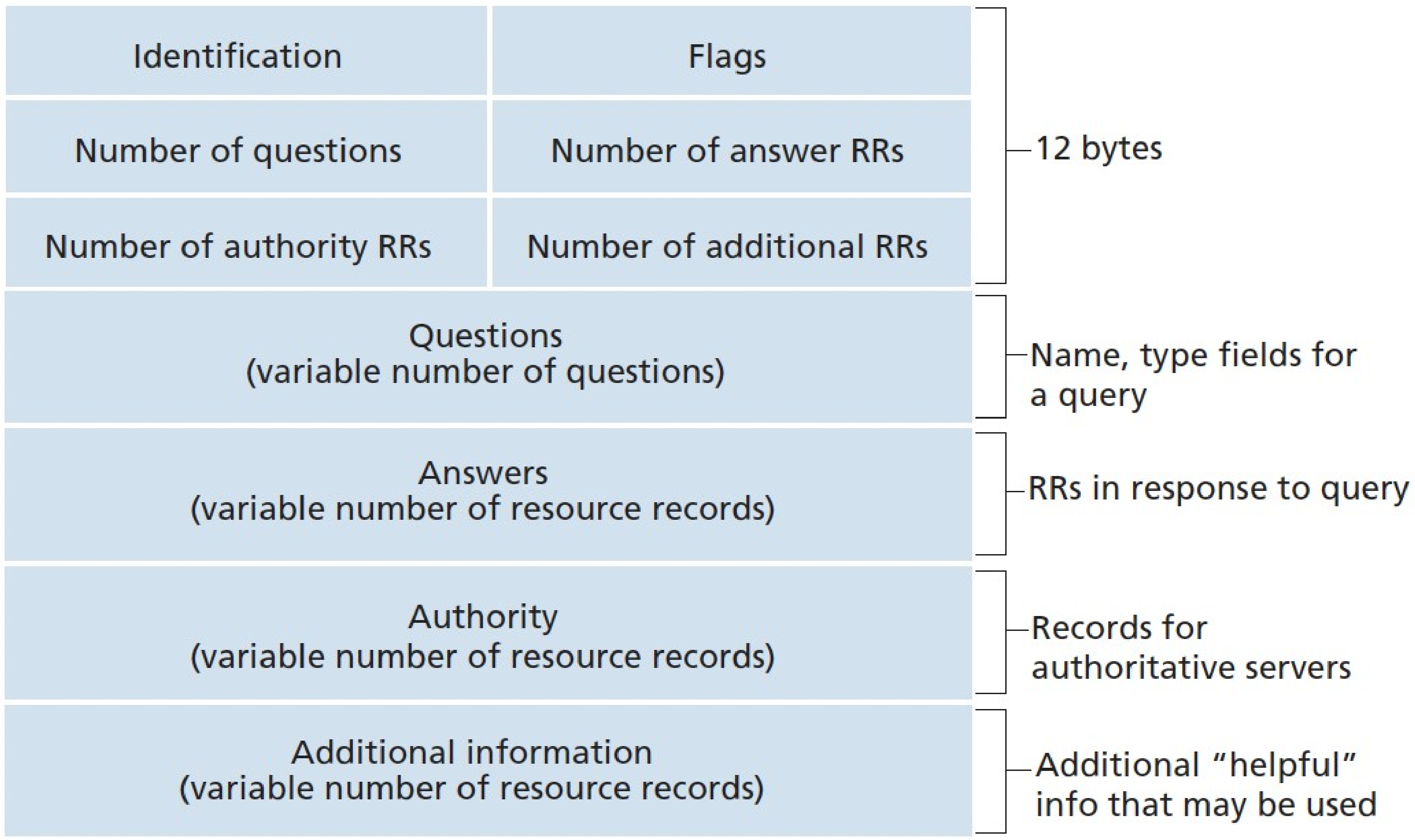
Resource Records

- If Type = CNAME
  - Value is a canonical hostname for the alias hostname Name
  - Can provide querying hosts the canonical name for a hostname
  - (foo.com, relay1.bar.foo.com, CNAME) is a CNAME record
- If Type = MX
  - Value is the canonical name of a mail server that has an alias hostname Name
  - (foo.com, mail.bar.foo.com, MX)
  - Allow hostnames of mail servers to have simple aliases
  - A company can have the same aliased name for its mail server and for one of its other servers
  - Obtain canonical name for the mail server, a DNS client would query for the MX record
  - Obtain canonical name for the other server, DNS client would query for the CNAME record

Other Thoughts…

- If a DNS server is authoritative for a particular hostname, DNS server will contain a Type A record for the hostname
- If a server is not authoritative for a hostname, then the server will contain a Type NS record for the domain that includes the hostname
  - Will also contain a Type A record that provides the IP address of the DNS server in the value field of the NS record

Figure 2.21 – DNS Message Format



DNS Messages

- Two kinds of messages: query and reply
  - Both have same format
- Semantics
  - First 12 bytes – header section
    - Query – 16-bit number
    - Identifier is copied into the reply message to a query, allowing the client to match received replies with sent queries
  - Flag field
    - 1-bit query/reply flag indicates whether the message is a query (0) or reply (1)
    - 1-bit authoritative flag is set in a replay when a DNS server is an authoritative server for a queried name
    - 1-bit recursion-desired flag set when a client desires that the DNS server perform recursion when it doesn’t have the record
    - 1-bit recursion-available field – set in a reply if DNS server supports recursion

DNS Messages

- Semantics
  - Header – there are also four number-of fields
    - Indicate the number of occurrences of the four types of data sections that follow the header
  - Question section – information about the query being made
    - Name field that contains the name that is being queried
    - Type field that indicates the type of question being asked about the name
      - Host address associated with a name (Type A)
      - Mail server for a name (Type MX)
  - Answer section – reply from a DNS server
    - Contains resource records for the name that was originally queried; can return multiple RRs in the answer, since a hostname can have multiple IP addresses
  - Authority section – records of other authoritative servers
  - Additional section – other helpful records
    - Example: answer field in a reply to an MX query contains a resource record providing the canonical hostname of a mail server; additional section contains a Type A record providing the IP address for the canonical hostname of the mail server

Inserting Records Into the DNS Database

- How to add? Example…
- Created a new start up called Network Utopia
- Register the domain name networkutopia.com at a registrar
  - Commercial entity that verifies the uniqueness of the domain name, enters the domain name into the DNS database and collects a small fee from you for its services
- When registering domain name, you also need to provide the registrar with the names and IP addresses of your primary and secondary authoritative DNS servers
  - Names: dns1.networkutopia.com, dns2.networkutopia.com
  - IP addresses: 212.2.212.1, 212.212.212.2
- For each of the authoritative servers, registrar would then make sure that a Type NS and Type A record are entered into the TLD com servers
- Inserts
  - (networkutopia.com, dns1.networkutopia.com, NS)
  - (dns1.networkutopia.com, 212.2.212.1, A)
- Make sure the Type A resource record for the web server and the Type MX resource record for your mail server are entered into your authoritative DNS servers