18CSC302J- Computer Networks

Unit-3

Syllabus

1. **DNS- DNS in the Internet, DNS Resolution, DNS Messages**
2. TELNET – SSH
3. FTP- TFTP
4. WWW Architecture, Documents
5. HTTP, HTTP Request and Reply,
6. DHCP Operation, DHCP Configuration
7. SMTP, POP3, IMAP, MIME

Learning Resources

1. Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006 ISBN: 0131876716, ISBN: 978-0131876712

DNS
(Domain Name System)

DNS

- TCP/IP protocols uses IP address.
- Identifies connection of a host to the internet.
- System maps a name to an address
- Host file – only two columns (name, address)
- Single host file – maps the names to address
- Host file would be large to store in every host.
- Impossible to update the changes happens every time to the host file.

Solution 1

- Store the host file in a single system and allow the centralized information access to every system that needs mapping.

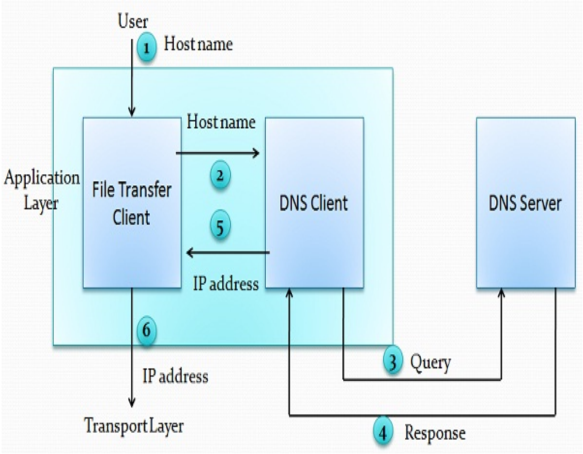
Disadvantage

- Huge amount of traffic to the internet.

Solution 2

- Divide the huge amount of information into smaller parts and store on different systems.
- Host which needs mapping can communicate to the closest system that holds the information.
- This solution is called Domain Name System.

Purpose of DNS



Six steps to map host name to an IP address

1. User passes the host name to the file transfer client (FTC).
2. FTC passes the host name to DNS client.
3. DNS client sends a message to the DNS Server. The query gives the file transfer server name using the known IP address of the DNS server.
4. DNS server responses back with the IP address of the desired file transfer server.
5. DNS client passes the IP address to file transfer server.
6. FTC uses the IP address it received to access the file transfer server.

Two Connections must be made

- Mapping the name to an IP address
- Transferring files

Namespace

- Maps the address to the unique names.
- Organized in two ways flat or hierarchical.

Flat Name Space

- Name is assigned to an address, name is the sequence of characters without structures.

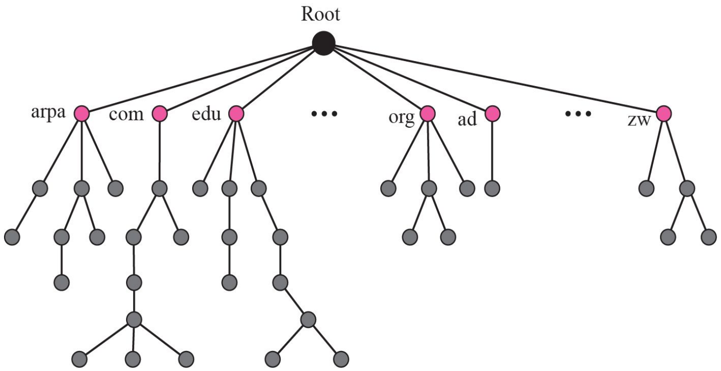
Disadvantage

- Cannot used in large system.
- Centrally controlled to avoid ambiguity and duplications.

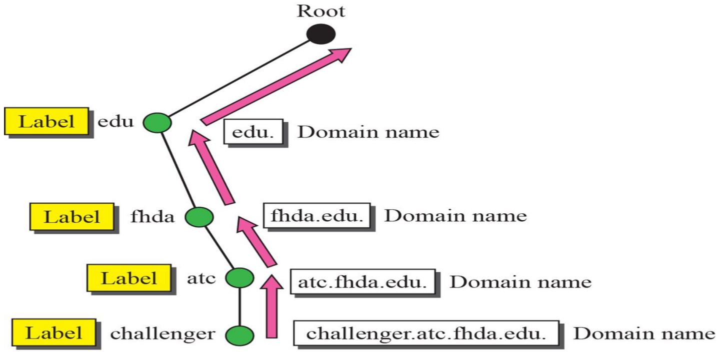
Hierarchical Name Space

- Each name is made up of several parts.
- First part – nature of organization
- Second part – name of an organization
- Third part – departments in the organization
- Namespace can be decentralized.
- Suffixes (or prefixes) are added to the name that defines the host or system.

Domain Name Space



Domain Name System



Domain names and labels

- ✔ Hierarchical name space – DNS was designed.
- ✔ Names are defined in inverted tree structure with root at top.
- ✔ Tree have 128 levels – 0 (root) to 127.

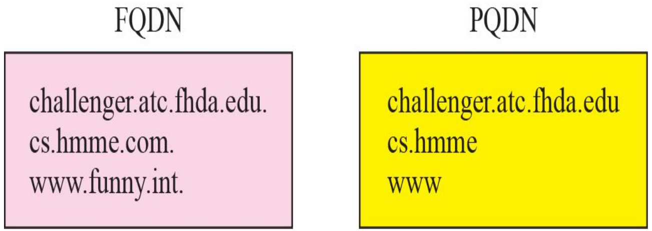
Label

- ✔ Each node in a tree has a label – max of 63 characters.
- ✔ Root label is a null string.
- ✔ Children node should have different labels that will ensure uniqueness in domain names.

Domain Name

- ✔ Full domain name is the sequence of labels separated by dots.
- ✔ Domain names read from nodes up to the root.
- ✔ Full domain name always ends in a null label.

Fully Qualified Domain Names (FQDN)
Partially Qualified Domain Names (PQDN)



FQDN

challenger.atc.fhda.edu.
cs.hmme.com.
www.funny.int.

PQDN

challenger.atc.fhda.edu
cs.hmme
www

FQDN and PQDN

Fully Qualified Domain Names (FQDN)

- If the label is terminated by null string it is called fully qualified domain names.
- Contains the full name of the host, contains all labels from most specific to most general.
- DNS server can match an FQDN to an address.

Eg: challenger.atc.srmuniv.edu.

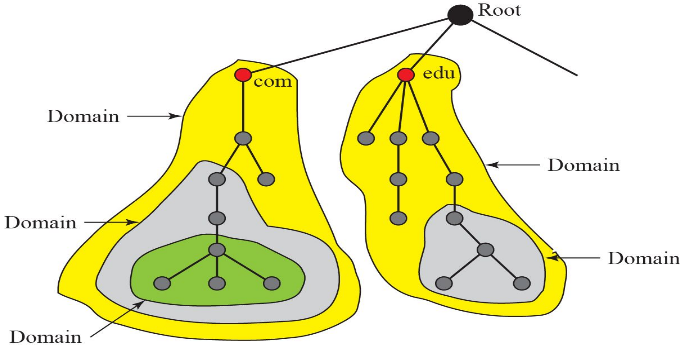
Partially Qualified Domain Names (PQDN)

- If the label is not terminated by null string it is called partially qualified domain name.
- PQDN starts from the node but does not reach the root.
- The resolver will supply the missing part called the suffix to create a PQDN.
- User at fhda.edu site wants to get the IP address of the challenger computer, has to mention the partial name.

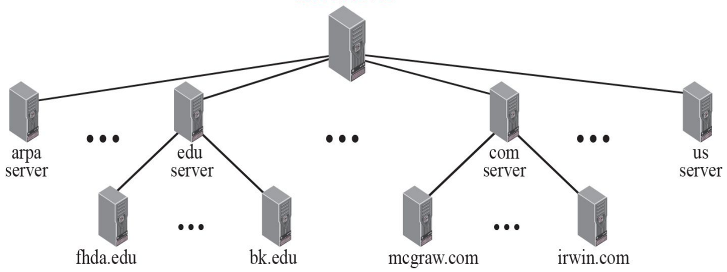
Eg: challenger

- The DNS client adds the suffix before parsing the address to the DNS server.

Domain Name Space



Domains



Hierarchy of name servers

Domain

- It is the subtree of domain name space.
- The domain is the name of the node at the top of the subtree.
- Domains may itself divided into sub domains.

Distribution of name space

- Information in the name space must be stored.
- It is inefficient and not reliable to store the information in a single system.

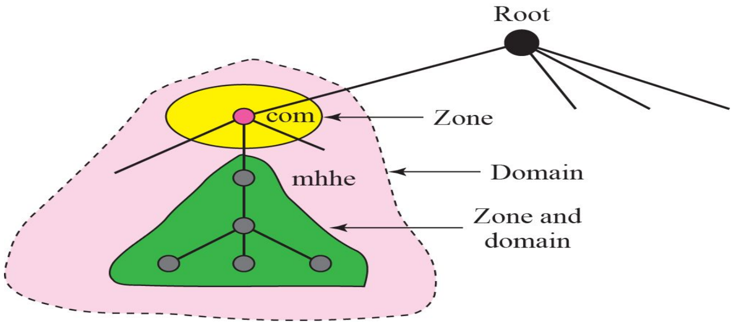
Solution

- Distribute the information among many computers called DNS servers.

Hierarchy of name space

- Divide the whole space into many domains based on the first level.

Domain Name Space



Zones and Domains

Zone

- What a server is responsible for or has authority over is called zones.
- Zone is the contiguous part of the entire tree.
- If server accepts the responsibility for a domain and does not divide the domain into smaller domains then “domain” and “zone” refers the same thing.

Root server

- It is the server whose zone consists of the whole tree.
- It does not store any information about the domains but delegates the authority to other servers, keeping references to those servers.

Domain Name Space

Primary and Secondary Servers

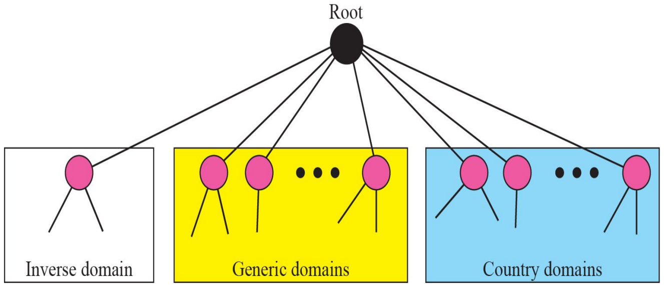
Primary Server

- Server that stores the file about the zone for which it is in authority.
- It is responsible for creating, maintaining and updating the zone files.
- It stores zone file on a local disk.

Secondary Servers

- Server that transfers the complete information about zone from another server and stores the file on its local disk.
- Secondary server neither creates nor updates the zone files.

DNS in the Internet



DNS used in internet

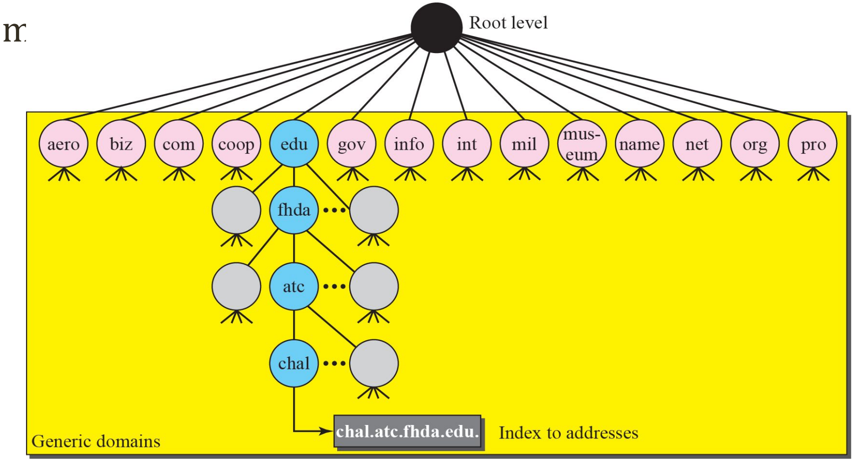
Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to “com”)
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Generic Domain Labels

- In internet the domain name space is divided into three different sections.
- Generic domains, country domains and the inverse domains.

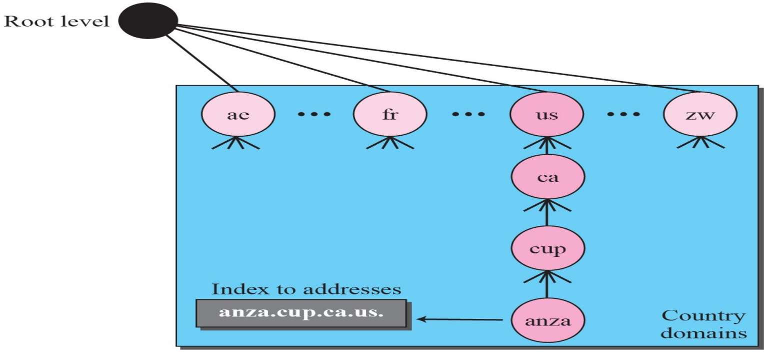
Generic Domains

- Define registered hosts according to their generic behaviour.
- Each node in a tree defines a domain which s an index to the dom

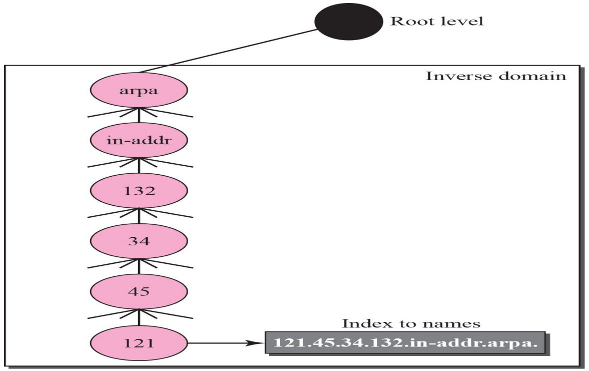


Generic Domains

DNS in the Internet



Country Domains



Inverse Domain

Country Domains

- Uses two character country abbreviations.

  Eg: US for United Sates

- Second label can be organizational or they can be more specific national designations.

  Eg: ca.us

Inverse Domain

- It is used to map an address to a name.
- This happens when the server has received a request from the client.
- Type of query called an inverse or pointer (PTR) query.
- To handle the pointer query the inverse domain is added to the domain name space with the first level node.

Resolution

Mapping a name to an address or an address to a name is called *name-address resolution*.

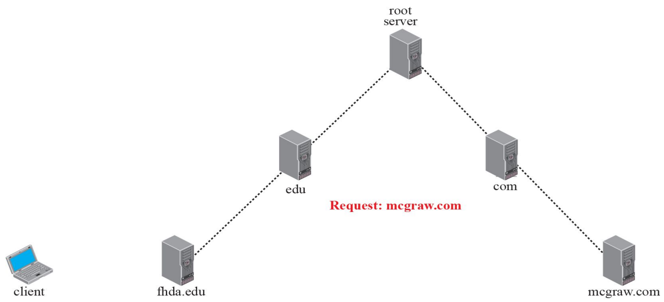
Resolver

- DNS is designed as a client – server application.
- Host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.
- After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error and finally delivers the results to the process that requested it.

Mapping Names to Addresses

- The resolver gives a domain name to the server and asks for the corresponding address.
- If the domain name is from the generic domain the resolver receives a domain name such as “chal.atc.fhda.edu.
- if the domain name is from the country domain the resolver receives a domain name such as “ch.fhda.cu.ca.us.

Resolution



Recursive resolution

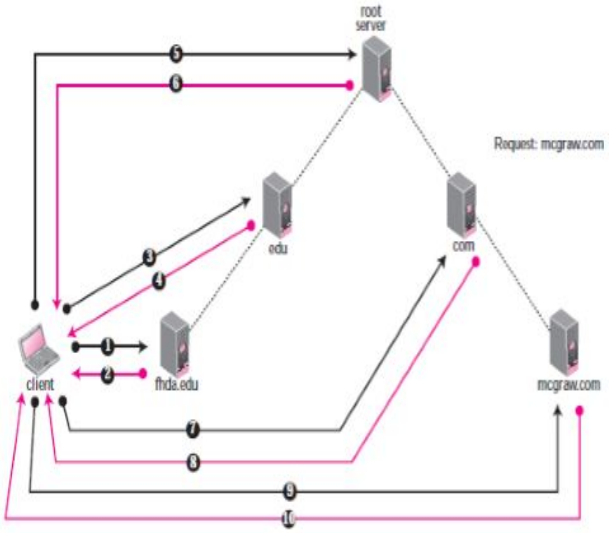
Mapping Addresses to Names

- A client can send an IP address to a server to be mapped to a domain name.
- To answer the PTR query DNS uses the inverse domain.
- in the request the IP address is reversed and two labels in-addr and arpa are appended to create a domain acceptable by the inverse domain.

Recursive Resolution

- The client can ask for a recursive answer from a name server.
- If the server is the authority for the domain name, it checks its database and responds.
- If the server is not the authority it sends the request to another server and waits for the response.
- If the parent is the authority it responds otherwise it sends the query to another server.

Resolution



Iterative Resolution

Iterative Resolution

- If server is an authority for the name it sends the answer.
- If not it returns the IP address of the server that thinks it can resolve the query.
- The client is responsible for repeating the request to the second server.
- The client repeats the same procedure to next server and so on
- This process is called **iterative** because the client repeats the same query to multiple servers.

Catching

- Each time the **server receives** the query for a name that is not in domain it needs to search its database for a server IP address.
- Reduction in search time would increase the efficiency.
- DNS handles this with the mechanism called **catching**

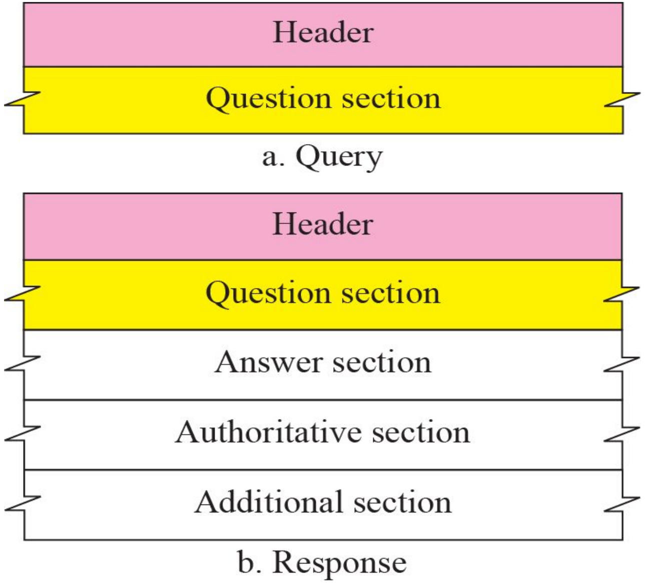
Resolution

- **Reduction of search** time would increase the **efficiency**.
- DNS handles this with the mechanism called **catching.**
- **Catching speeds up** resolution but it can also **be problematic**.
- If the server **catches the mapping** for a long time it may send an **outdated mapping to the client**.

Two counter techniques are used

- The authoritative server always adds information to the mapping called **time to live**.
- DNS requires each server keep a **TTL counter** for each mapping it caches.

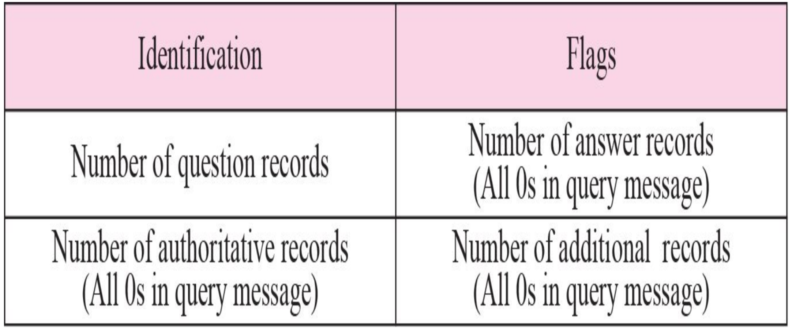
DNS Messages



Query and Response Messages

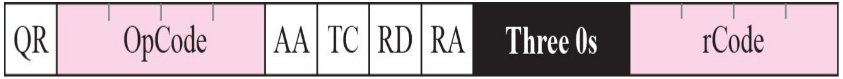
- DNS messages are of two types
    - Query
    - Response
- The query message consists of header and question records.
- The response message consists of header, question records, answer records, authoritative records and additional records.

DNS Messages



Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Header Format



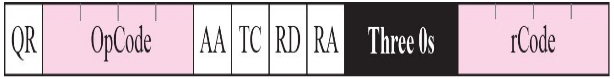
QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

Flags Field

Header

- Both query and response message have the same header format with some fields set to zero for query messages.
- The header is of 12 bytes.
- Identification - 16 bit field used by client to match the response with the query.
- Flags – 16 bit field consisting of the subfields.
- QR (Query/Response) – 1 bit sub field defines type of message.
  0 – message is query
  1 – message is response
- OpCode - 4 bits, defines the type of query or response
  0 – standard
  1 – inverse
  2 – server status request

DNS Messages



Flags Field

- AA (Authoritative Answer) – 1 bit subfield

  Set to 1 - name server is the authoritative server

  Used only in response message.

- TC (Truncate) – 1 bit subfield

  Set to 1 – response was more than 512 bytes and truncated

  It is used when DNS uses the services of UDP

- RD (Recursion Desired) – 1 bit subfield

  Set to 1 – client desires a recursive answer

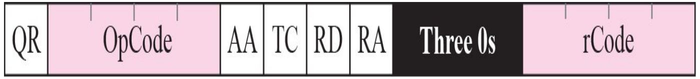
  It is set in query message and repeated in the response message

- RA (Recursion Available) – 1 bit subfield

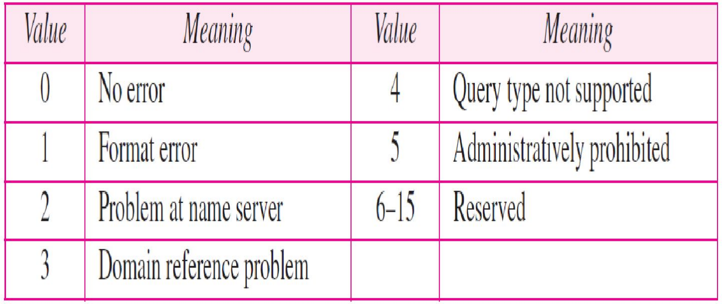
  Set in response, means that a recursive response is available

  Set only in response message

DNS Messages



Flags Field



Value	Meaning	Value	Meaning
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6–15	Reserved
3	Domain reference problem		

Values of rcode

- Reserved – 3 bit sub field set to 000.
- rcode – 4 bit field shows status of error in response

  Only authoritative server can make the judgement
- Number of question records – 16 bit field

  Contains the number of queries in question section of the message
- Number of answer records – 16 bit field

  Contains the number of answer records in answer section of the response message
- Number of authoritative records – 16 bit field

  Contains number of authoritative records in authoritative section of the response message

  It's value is zero in query message
- Number of additional records – 16 bit field

  Contains number of additional records in additional section of a response message

DNS Messages

- Question Section

  Consists of one or more question records

  It is present in both query and response messages

- Answer Section

  Consists of two or more resource records

  It is present only on response messages

- Authoritative Section

  Consists of two or more resource records

  It is present only on response messages

  Gives information (domain name) about one or more authoritative servers for the query

- Additional Information Section

  Consists of two or more resource records

  It is present only on response messages

  Gives additional information that helps the resolver

DNS-SUMMARY

Need for DNS

- Purpose of DNS

Name space

- Flat name space
- Hierarchical name space
- Label
- Domain name
  - Fully Qualified Domain Name (FQDN)
  - Partially Qualified Domain Name (PQDN)
- Domain
- Distribution of name space
  - Hierarchy of name servers
  - Zone
  - Root server
  - Primary and secondary servers

DNS in the internet

- Generic domains
- Country domains
- Inverse domain

Resolution

- Resolver
- Mapping Names to Addresses
- Mapping Addresses to Name
- Recursive resolution
- Iterative resolution
- Caching

DNS Messages

- Query and Response