FOUNDATION OF WEB DEVELOPMENT

Domain Name System (DNS)

Purpose of naming

- Addresses are used to locate objects

- Names are easier to remember than numbers

- You would like to get to the address or other objects using a name

- **DNS provides a mapping from names to resources of several types**

Jump to first page

Names and addresses in general

- An address is how you get to an endpoint
  - Typically, hierarchical (for scaling):
    - 950 Charter Street, Redwood City CA, 94063
    - 204.152.187.11, +1-650-381-6003

- A “name” is how an endpoint is referenced
  - Typically, no structurally significant hierarchy
    - “David”, “Tokyo”, “itu.int”

DNS

- A lookup mechanism for translating objects into other objects
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
  - A “name space”
  - Servers making that name space available
  - Resolvers (clients) which query the servers about the name space

Jump to first page

Exercise

- Is DNS security critical?
- What would happen if it is not:
  - Confidential?
  - High integrity?
  - Available?

DNS Features: Global Distribution

- Data is maintained locally, but retrievable globally
  - No single computer has all DNS data
- DNS lookups can be performed by any device
- Remote DNS data is locally cachable to improve performance

Jump to first page ⇦ ⇨

DNS Features: Loose Coherency

- The database is always internally consistent
  - Each version of a subset of the database (a zone) has a serial number
    - The serial number is incremented on each database change
    - However, client does not know current number for zone apriori
- Changes to the master copy of the database are replicated according to timing set by the zone administrator
- Cached data expires according to timeout set by zone administrator

Jump to first page

DNS Concepts

- Next slides are about concepts

- After this set of slides you should understand
  - How the DNS is built
  - Why it is built the way it is
  - The terminology used throughout the course

Concept: DNS Names 1

- The namespace needs to be made hierarchical to be able to scale.
- The idea is to name objects based on
  - location (within country, set of organizations, set of companies, etc)
  - unit within that location (company within set of company, etc)
  - object within unit (name of person in company)

Concept: DNS Names 2
How names appear in the DNS

Fully Qualified Domain Name (FQDN)

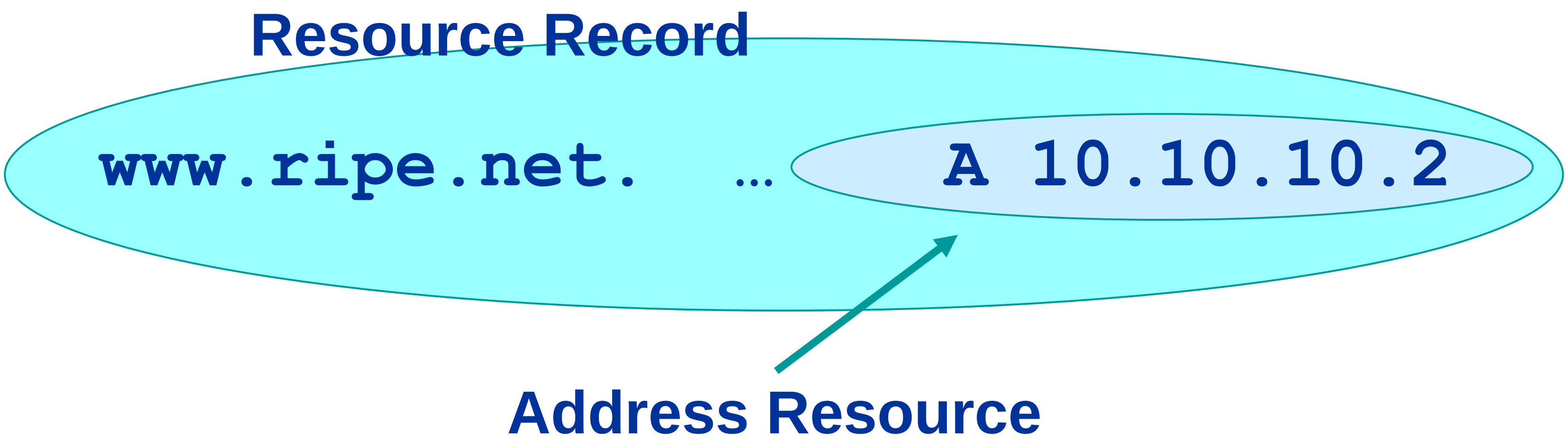
WWW.RIPE.NET.

Note the trailing dot

- labels separated by dots
- DNS provides a mapping from FQDNs to resources of several types
- Names are used as a key when fetching data in the DNS

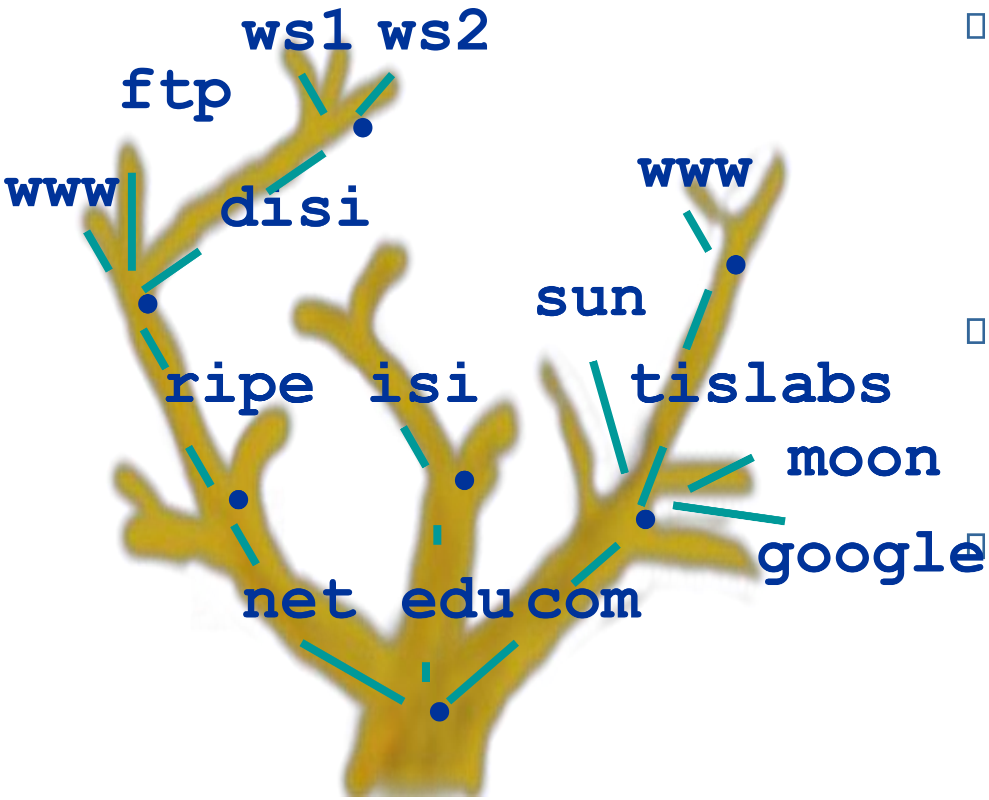
Concept: Resource Records

- The DNS maps names into data using Resource Records.



Jump to first page

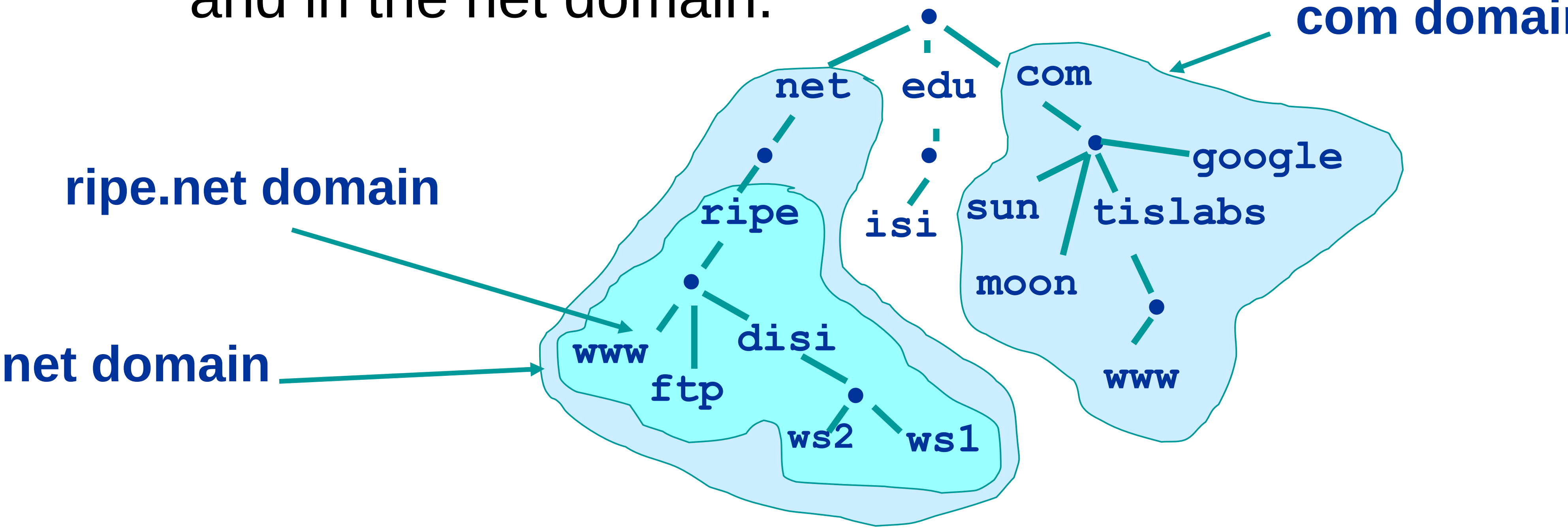
DNS Name Hierarchy



- Domain names can be mapped to a tree.
- New branches at the ‘dots’
- No restriction to the amount of branches.

Concept: Domains

- Domains are “namespaces”
- Everything below .com is in the com domain.
- Everything below ripe.net is in the ripe.net domain and in the net domain.


com domai
ripe.net domain
net domain

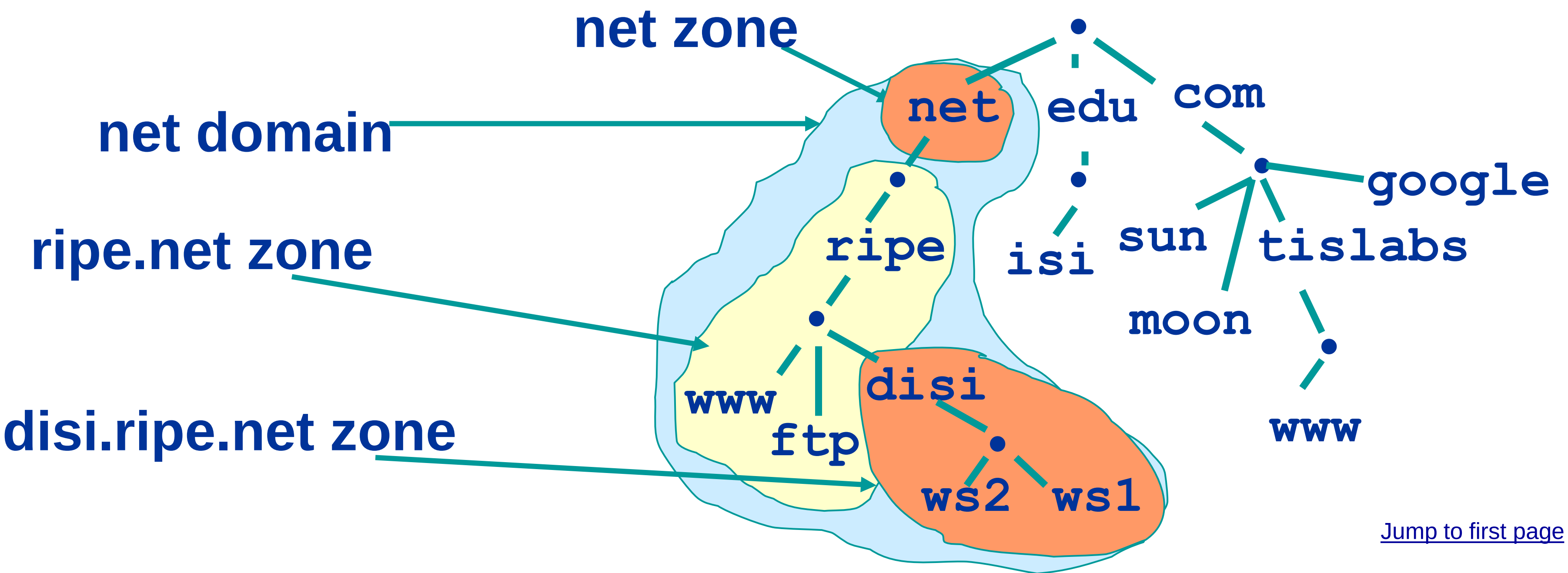
Jump to first page

Delegation

- Administrators can create subdomains to group hosts
  - According to geography, organizational affiliation or any other criterion
- An administrator of a domain can delegate responsibility for managing a subdomain to someone else
  - But this isn't required
- The parent domain retains links to the delegated subdomain
  - The parent domain "remembers" who it delegated the subdomain to

Concept: Zones and Delegations

- Zones are “administrative spaces”
- Zone administrators are responsible for portion of a domain’s name space
- Authority is delegated from a parent and to a child



Jump to first page

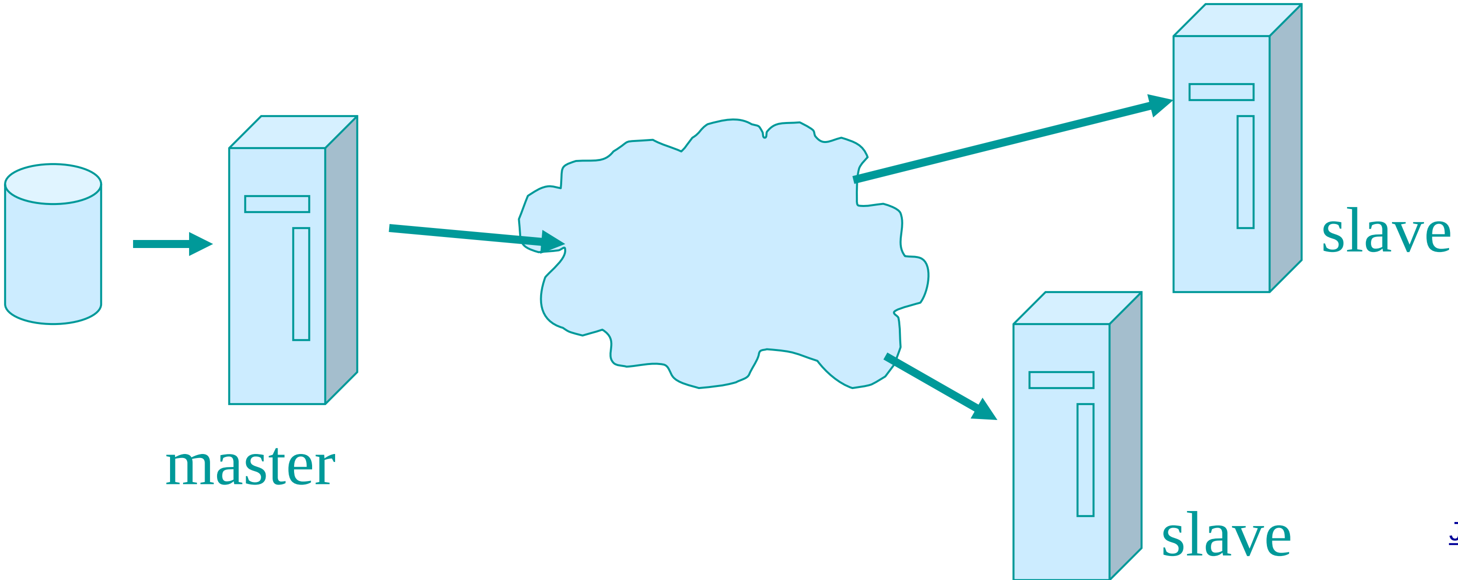
Name Servers

- Name servers answer ‘DNS’ questions.

- Several types of name servers
  - Authoritative servers
    - master (primary)
    - slave (secondary)
  - (Caching) recursive servers
    - also caching forwarders
  - Mixture of functionality

Authoritative name servers

- Give authoritative answers for one or more zones.
- The master server normally loads the data from a zone file
- A slave server normally replicates the data from the master via a zone transfer



Recursive Name Servers

- Recursive servers do the actual lookups; they ask questions to the DNS on behalf of the clients.

- Answers are obtained from authoritative servers but the answers forwarded to the clients are marked as not authoritative

- Answers are stored for future reference in the cache

Jump to first page ⇦ ⇨

Concept: Resolvers

- Resolvers ask the questions to the DNS system on behalf of the application.

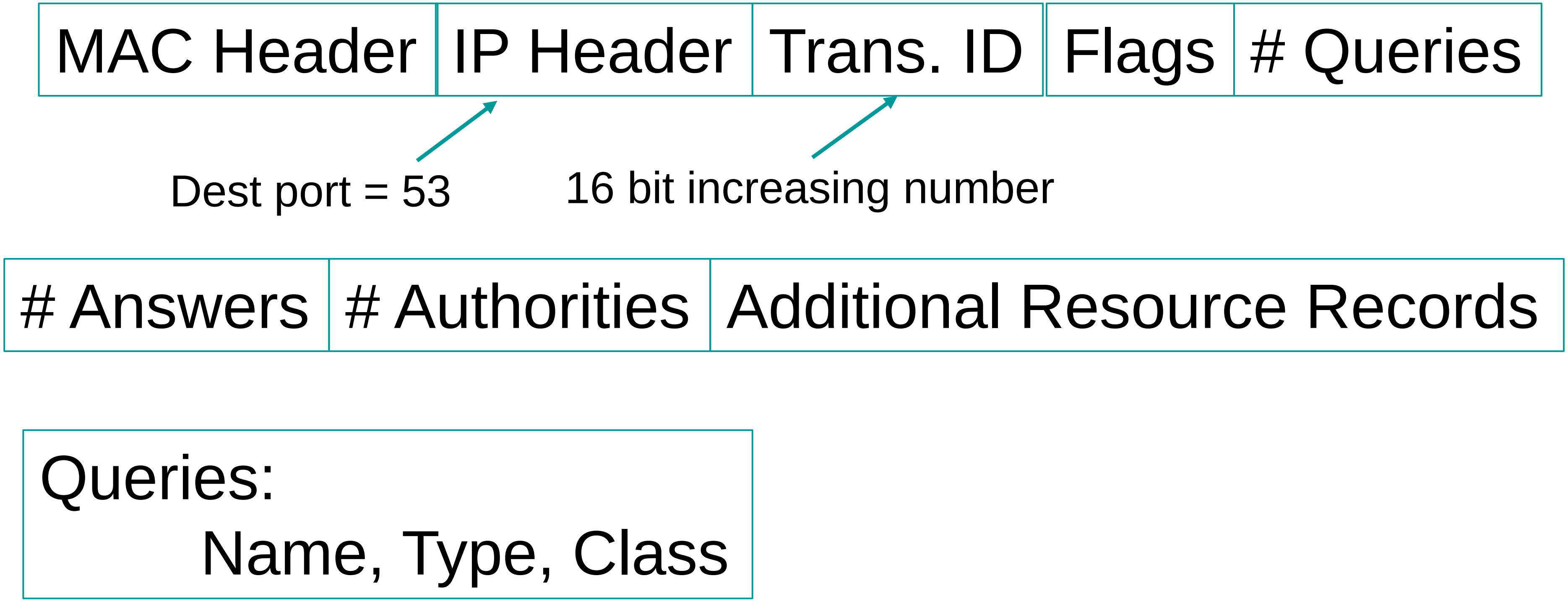
- Normally implemented in a system library (e.g, libc)

```
gethostbyname(char *name);
gethostbyaddr(char *addr, int len,
  type);
```

Jump to first page ⇦ ⇨

DNS Query Format

- Operates over UDP, destination port is 53



MAC Header | IP Header | Trans. ID | Flags | # Queries

Dest port = 53

16 bit increasing number

# Answers | # Authorities | Additional Resource Records

Queries:
Name, Type, Class

Jump to first page

DNS Flags

- 16 bits that identify the type of DNS record
  - Bit 1: query or response
  - Bit 2-5:Standard or inverse (lookup name of IP addr)
  - Bit 6: Is answer authoritative
  - Bit 7: Truncation
  - Bit 8: Query recursively
  - Bit 9: recursion available
  - Bits 10/12: reserved
  - Bit 11: Authority was auth. by sending server
  - Bits 13-16: error reporting

Jump to first page

Types of resolvers

- Root servers
- TLD servers
- Resellers
- Individual Domains
- Internet Registries (must be ICANN registered)

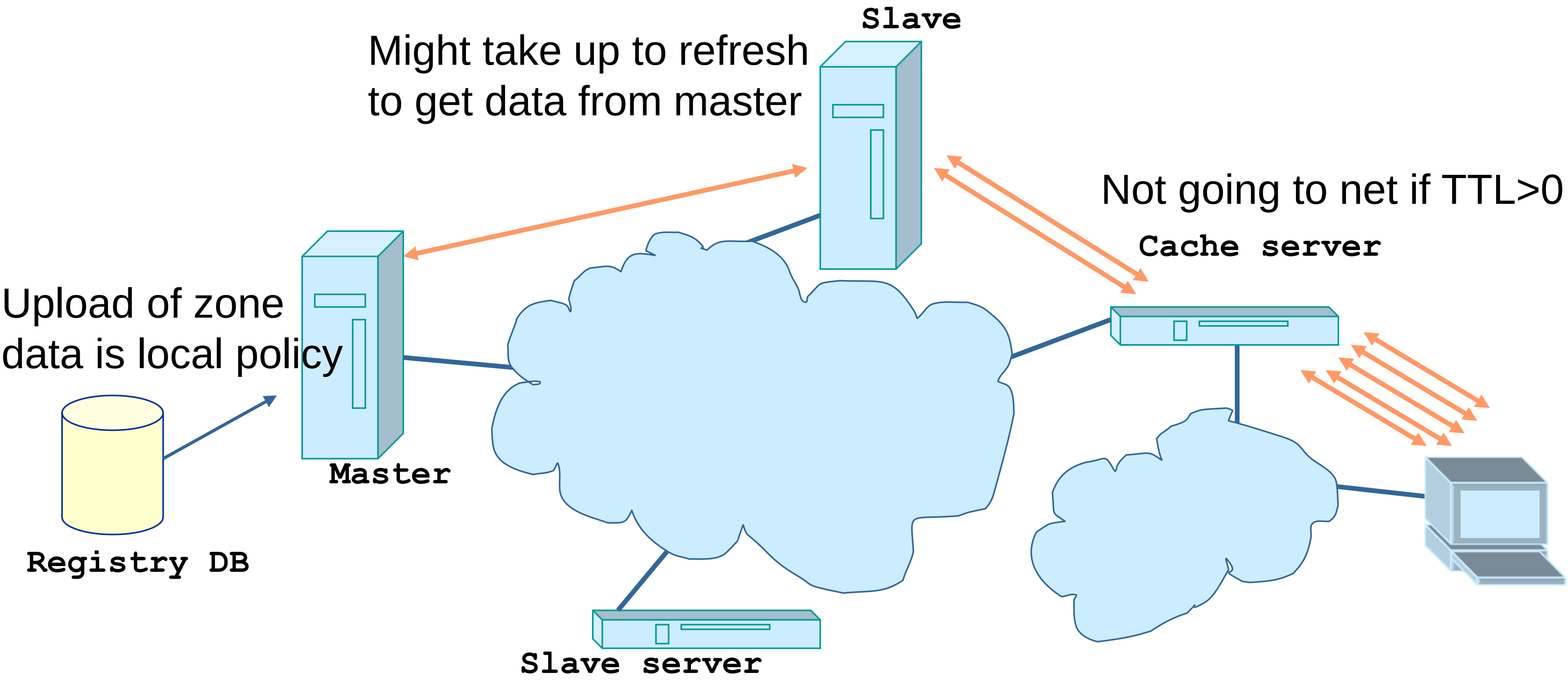
Requirements for registration

- Satisfy top-level requirements
  - E.g. for .ca must be Canadian person, business, or organization
- Claim to the domain (WWF vs WWE)
  - First come first serve
- Must verify ownership of IP resources/name server resources
- Sign registrant agreement
- Authorization code (if transferring)

Jump to first page

Places where DNS data lives

Changes in DNS do not propagate instantly!



Might take up to refresh to get data from master

Not going to net if TTL>0

Upload of zone data is local policy

DNS Features: Scalability

- No limit to the size of the database
  - One server has over 20,000,000 names
    - Not a particularly good idea
- No limit to the number of queries
  - 24,000 queries per second handled easily
- Queries distributed among masters, slaves, and caches

Jump to first page

DNS Features: Reliability

- Data is replicated
  - Data from master is copied to multiple slaves
- Clients can query
  - Master server
  - Any of the copies at slave servers
- Clients will typically query local caches
- DNS protocols can use either UDP or TCP
  - If UDP, DNS protocol handles retransmission, sequencing, etc.

Jump to first page

DNS Features: Dynamicity

- Database can be updated dynamically
  - Add/delete/modify of any record

- Modification of the master database triggers replication
  - Only master can be dynamically updated
    - Creates a single point of failure

Jump to first page