Introduction to the DNS system

Olaf M. Kolkman

Okolkman@ripe.net

Purpose of naming

- Addresses are used by routers, switches, and networking devices ….to locate hosts (computers, routers,..) but difficult to remember.
- Names are easier to remember than numbers
- **DNS provides a mapping from a domain name to an IP address.**

  Domain name: dantri.com.vn

  IP: 222.255.27.51

Naming History

- 1970's ARPANET
  - Host.txt maintained by the SRI-NIC
  - pulled from a single machine
  - Problems
    - traffic and load
    - Name collisions
    - Inconsistency
- DNS reated in 1983 by Paul Mockapetris (RFCs 1034 and 1035), modified, updated, and enhanced by a myriad of subsequent RFCs

DNS

- A globally distributed, loosely coherent, scalable, reliable, dynamic database to lookup translation from IP to domain names and vice versa.

- Comprised of three components
  - A “name space”
  - Servers making that name space available
  - Resolvers (clients) which query the servers about the name space

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

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
- 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

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

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.

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

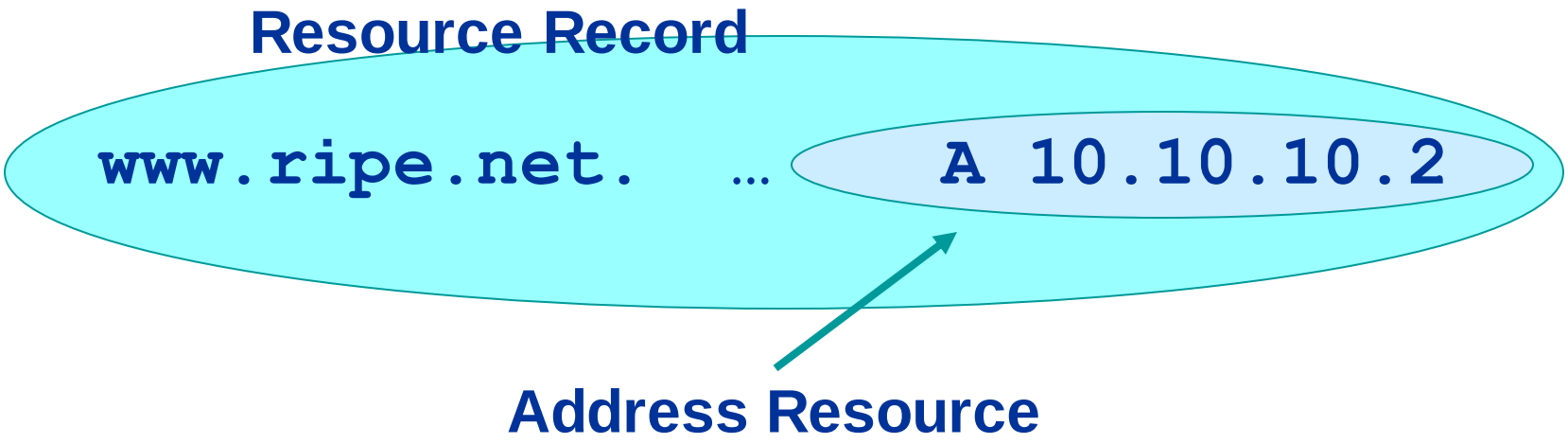
Fully Qualified Domain Name (FQDN)

WWW.RIPE.NET.

- 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

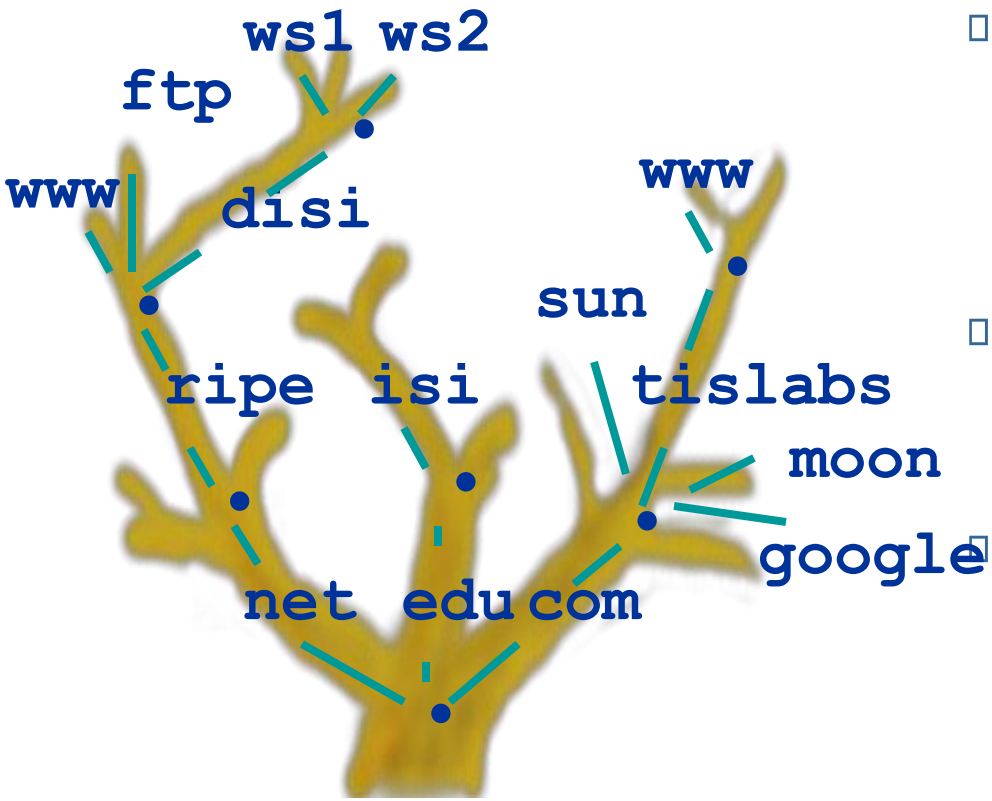
Concept: Resource Records

- The DNS maps names into data using Resource Records.



- More detail later

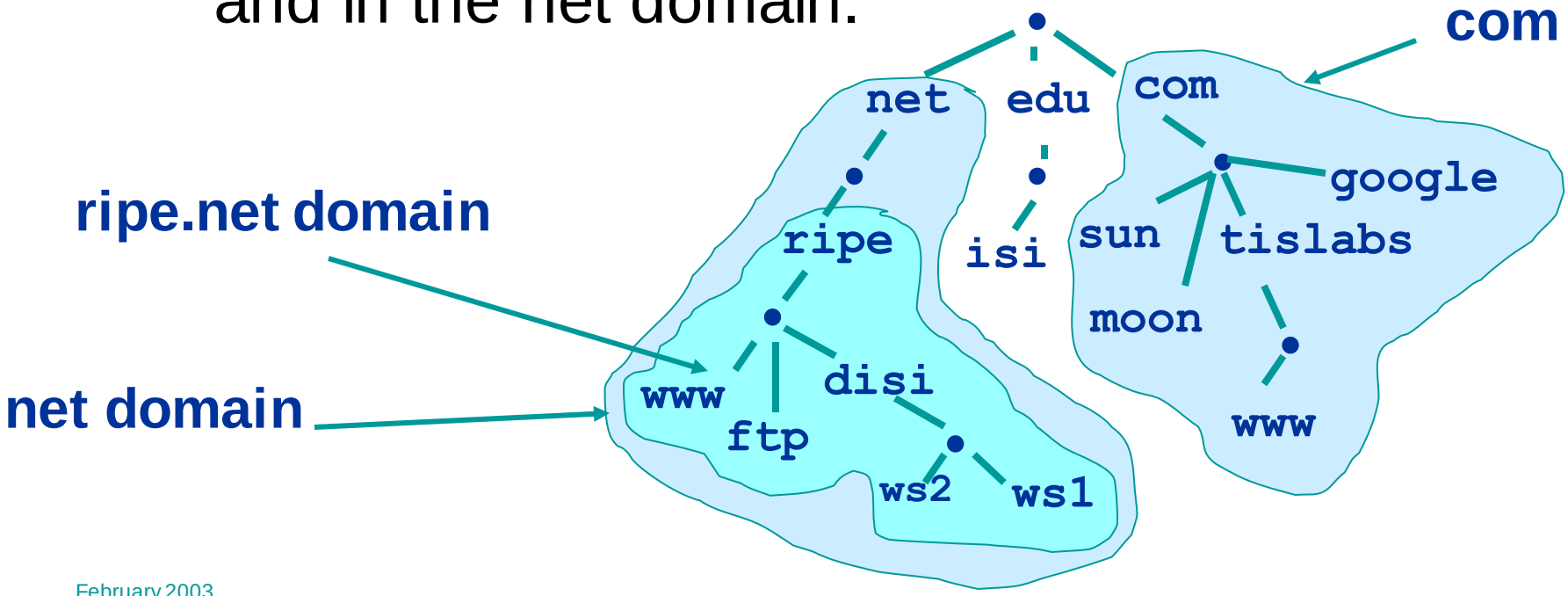
Concept: DNS Names 3



- 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.

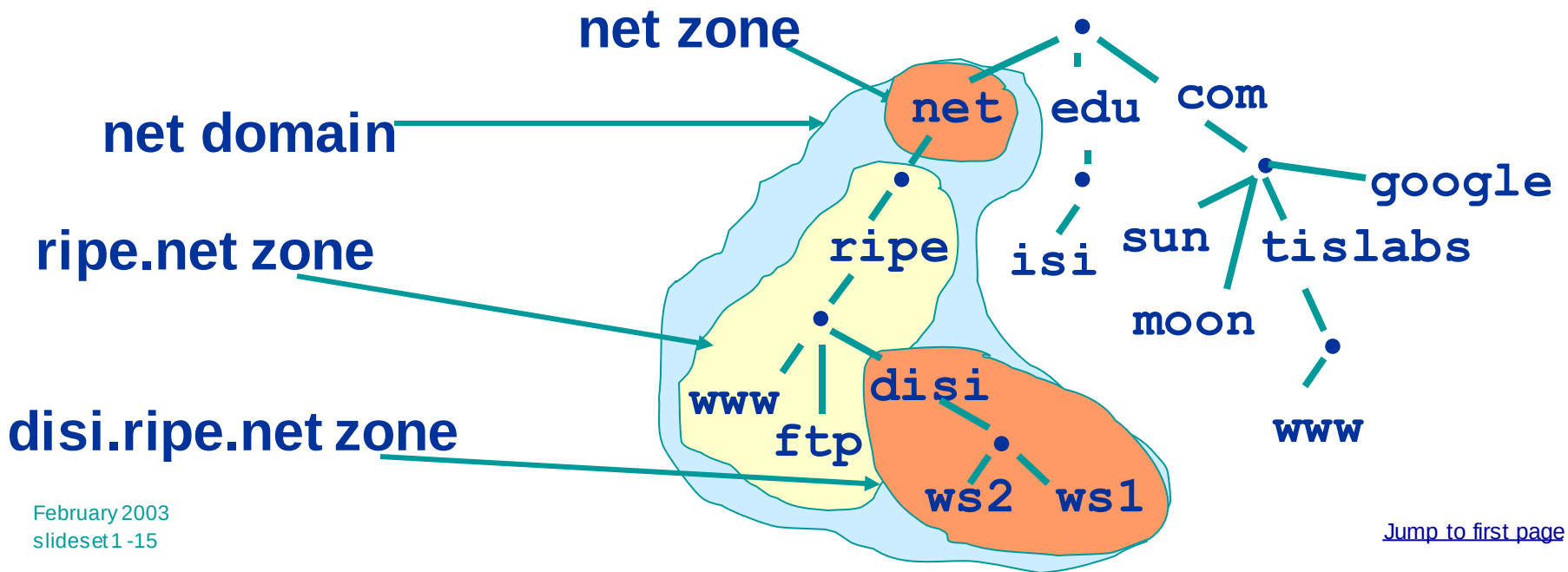


Delegation

- Administrators can create subdomains to group hosts
  - According to geography, organizational affiliation or any other criterion
- 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



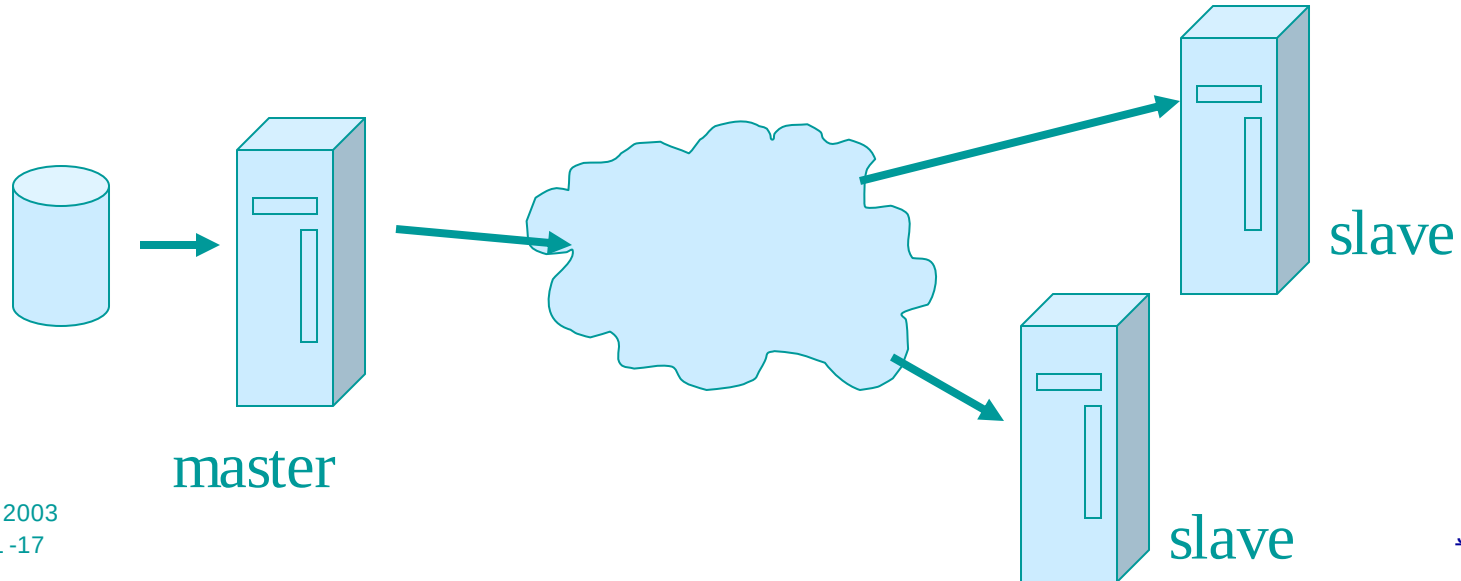
Jump to first page

Concept: 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

Concept: Name Servers authoritative name server

- 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



Concept: Name Servers recursive server

- 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

Concept: Resolvers

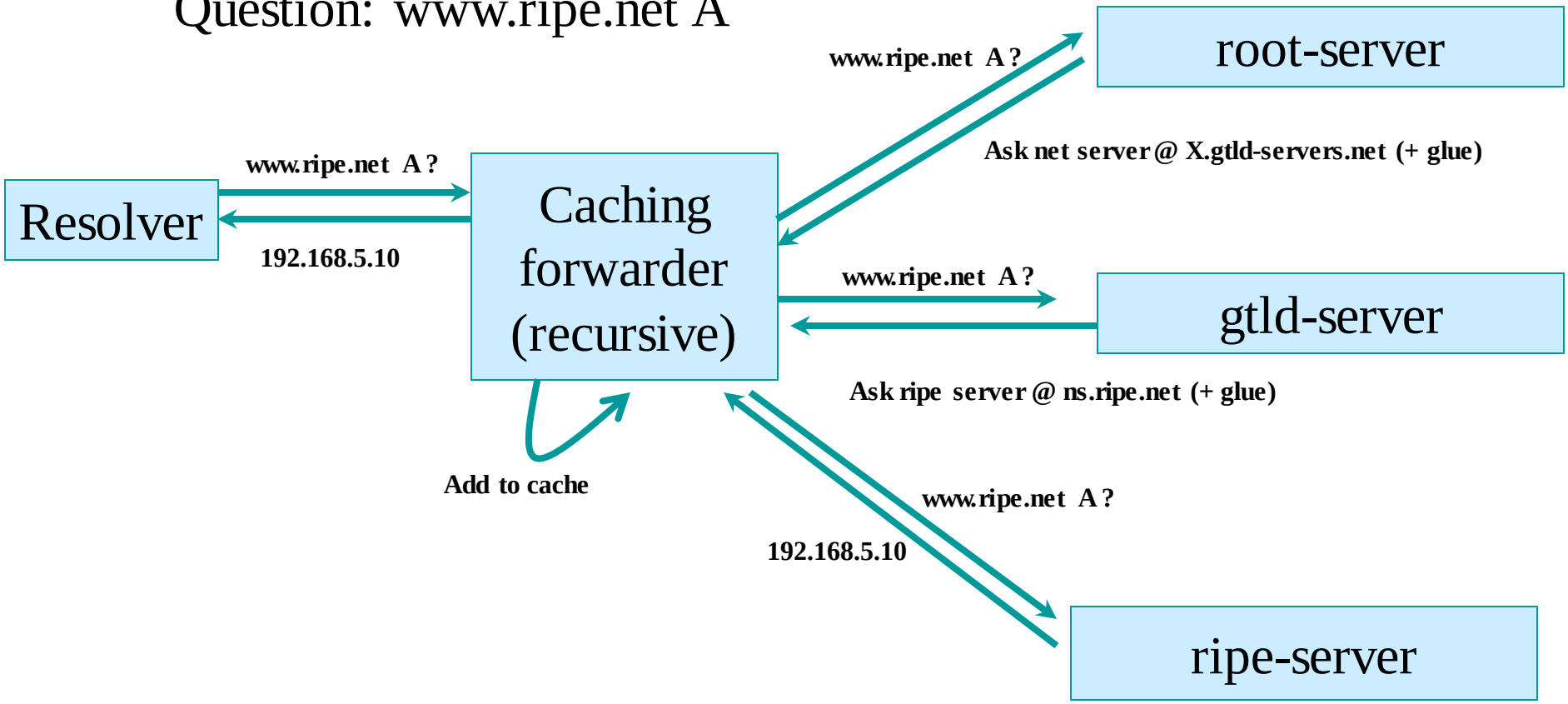
- Resolvers ask the questions to the DNS system on behalf of the application.

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

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

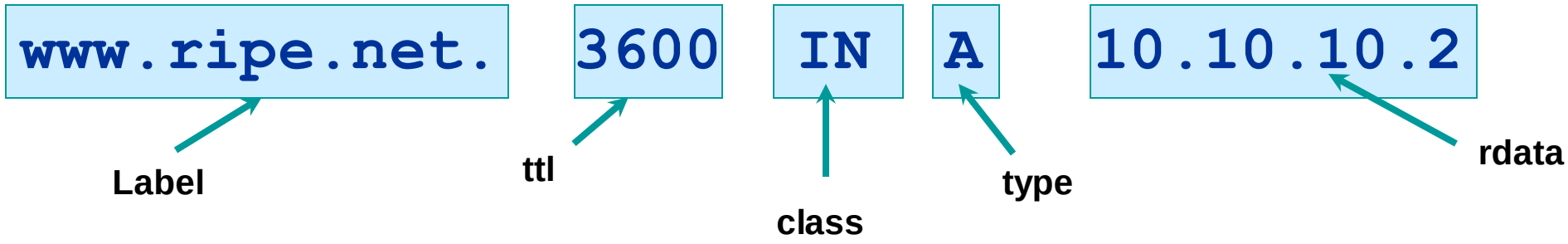
Concept: Resolving process & Cache

Question: www.ripe.net A



Concept: Resource Records (more detail)

- Resource records consist of it's name, it's TTL, it's class, it's type and it's RDATA
- TTL is a timing parameter
- IN class is widest used
- There are multiple types of RR records
- Everything behind the type identifier is called rdata



Example: RRs in a zone file

```
ripe.net. 7200 IN      SOA     ns.ripe.net.    olaf.ripe.net. (
                                2001061501      ; Serial
                                43200   ; Refresh 12 hours
                                14400   ; Retry 4 hours
                                345600  ; Expire 4 days
                                7200 ; Negative cache 2 hours
                        )
ripe.net. 7200  IN    NS      ns.ripe.net.
ripe.net. 7200  IN    NS      ns.eu.net.

pinkje.ripe.net. 3600  IN    A       193.0.1.162
host25.ripe.net. 2600  IN    A       193.0.3.25
```

Label ttl class type rdata

Jump to first page

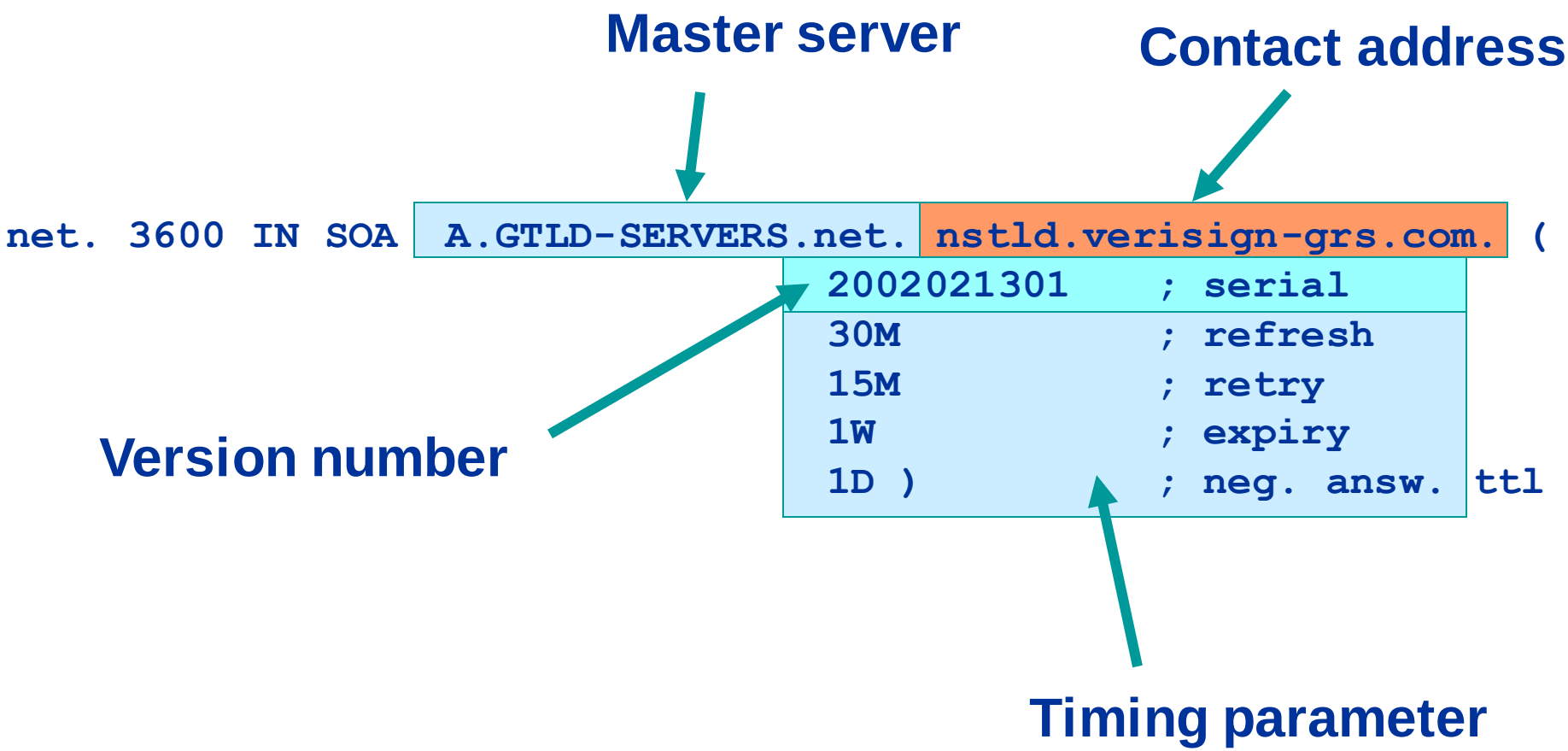
Resource Record: SOA and NS

- The SOA and NS records are used to provide information about the DNS itself.
- The NS indicates where information about a given zone can be found:

```
ripe.net.  7200   IN    NS      ns.ripe.net.
ripe.net.  7200   IN    NS      ns.eu.net.
```

- The SOA record provides information about the start of authority, i.e. the top of the zone, also called the APEX.

Resource Record: SOA

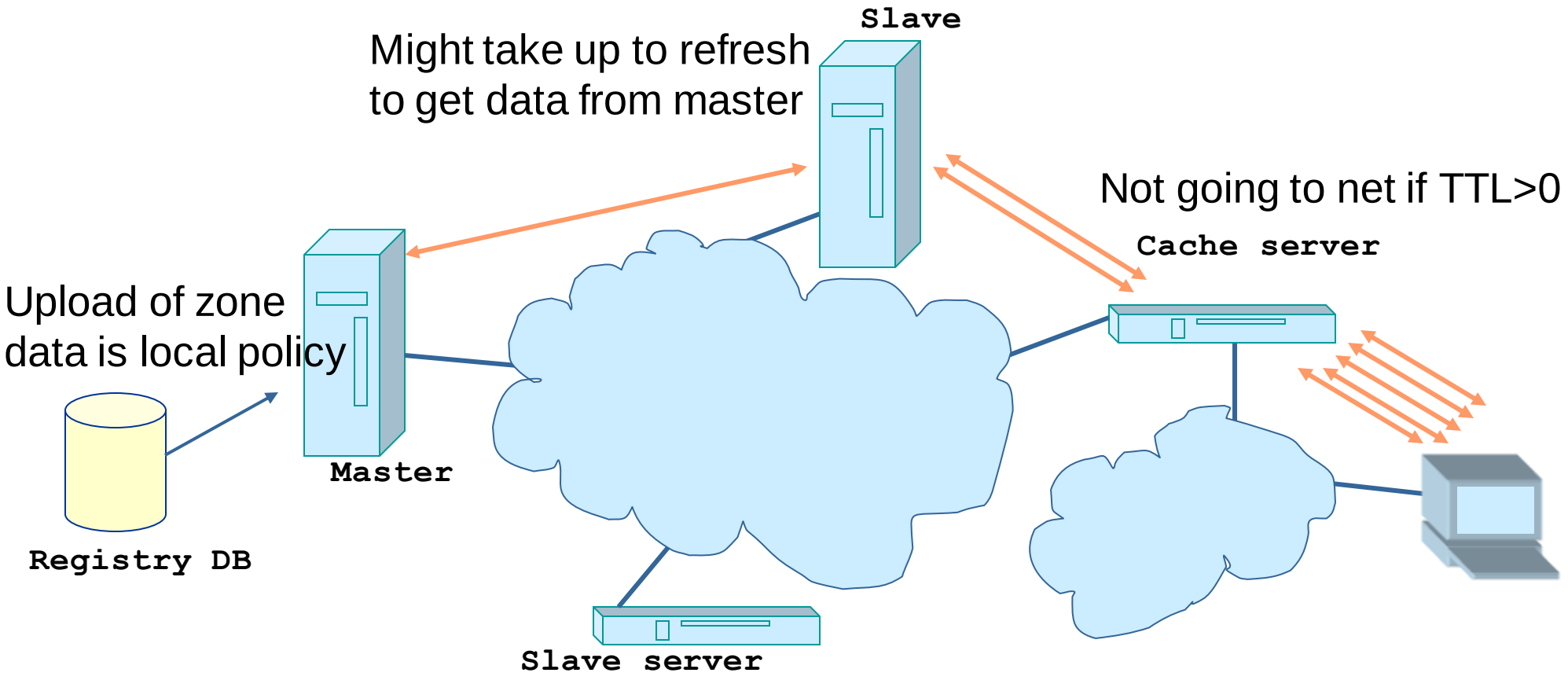


Concept: TTL and other Timers

- TTL is a timer used in caches
  - An indication for how long the data may be reused
  - Data that is expected to be ‘stable’ can have high TTLs
- SOA timers are used for maintaining consistency between primary and secondary servers

Places where DNS data lives

Changes in DNS do not propagate instantly!



Types of DNS records

- Important categories of data stored in DNS include the following:
  - An **A record** or **address record** maps a hostname to a 32-bit IPv4 address.
  - An **AAAA record** or **IPv6 address record** maps a hostname to a 128-bit IPv6 address.
  - A **CNAME record** or **canonical name record** is an *alias* of one name to another
    - The A record to which the alias points can be either local or remote - on a foreign name server.
    - This is useful when running multiple services (like an FTP *and* a webserver) from a single IP address.
    - Each service can then have its own entry in DNS (like ftp.example.com. and www.example.com.)
  - An **MX record** or **mail exchange record** maps a domain name to a list of mail exchange servers for that domain.
  - A **PTR record** or **pointer record** maps an IPv4 address to the canonical name for that host.
    - Setting up a PTR record for a hostname in the in-addr.arpa. domain that corresponds to an IP address implements reverse DNS lookup for that address.
    - For example (at the time of writing), www.icann.net has the IP address 192.0.34.164, but a PTR record maps 164.34.0.192.in-addr.arpa to its canonical name, referrals.icann.org.
  - An **NS record** or **name server record** maps a domain name to a list of DNS servers authoritative for that domain.
    - Delegations depend on NS records.

Example DNS Record for logicbbs.org

```
IN NS ns.planix.com
IN NS ns1.mydyndns.org
IN NS ns2.mydyndns.org

IN MX 10 mail
IN A 69.17.158.109

www IN A 69.17.158.109
mail IN A 69.17.158.109
```

- First three lines describe valid name servers for logicbbs.org.
- Following two entries indicate that the mail exchanger for logicbbs.org has a priority of 10 and messages should be directed to mail.logicbbs.org.
- Priority values indicate where to send e-mail if a server is unavailable; the lower the priority value, the higher the priority of that server.
  - Mail servers send e-mail to the server with the lowest priority value, and then work their way up the values listed as necessary.
- The last two lines indicate that logicbbs.org (the second-level domain) points to 69.17.158.109.
  - The www and mail subdomains (www.logicbbs.org, mail.logicbbs.org) also point to 69.17.158.109.
- The DNS record is the reason why some internet addresses do not need the www prefix, while others do.
  - If that particular domain has a www A record that differs from the basic A record, then anydomain.com may be different from *www*.anydomain.com, and the former may not work.
  - Other sites, like logicbbs.org, have both the top-level domain and the www subdomain pointing to the same IP address, which reduces confusion and ambiguity