Plain Old DNS

Presented by

Olaf Kolkman (NLnet Labs)

and

Alain Aina (TRS)

Rabat, Morroco, June 1, 2008

Presentation Road Map

- Why a naming system
- DNS Components
- DNS Features
- Techie details

IP: Identifiers on the Internet

- The fundamental identifier on the internet is an IP address.
- Each host connected to the Internet has a unique IP address
  - IPv4 or IPv6
  - Uniqueness guaranteed through allocation from one single pool

How Devices use Identifiers

- On operating system level only the numbers matter
- Terminology in this context
  - TCP/IP Stack
  - Sockets
- The devices do not care about names

What is easier to remember?

- Humans tend to remember names better, easier to associate

NL 1098VA 419 or Kruislaan 419, Amsterdam, Netherlands

89 GH 23 or Olaf's Ford Focus

213.154.224.1 or www.nlnetlabs.nl

host.txt

- In the1970's ARPA net, tables where maintained mapping host-names to IP addresses
  - SRI-NIC
  - Tables were pulled from the single machine
  - Problems
    - traffic and load
    - Name collisions
    - Consistency

DNS

- Domain Name System provides a scalable, distributed lookup mechanism.
- DNS created in 1983 by Paul Mockapetris
  - RFCs 882 and 883
- IETF Full Standard: RFCs 1034 and 1035 (1987)
  - modified, updated, and enhanced
  - DNS Security extensions being the most recent

Presentation Road Map

- Why a naming system
- DNS Components
- DNS Features
- Techie details

The four components

- A “name space”
- Servers making that name space available
- Resolvers (clients) which query the servers about the name space
- The protocol
  - Glues all together

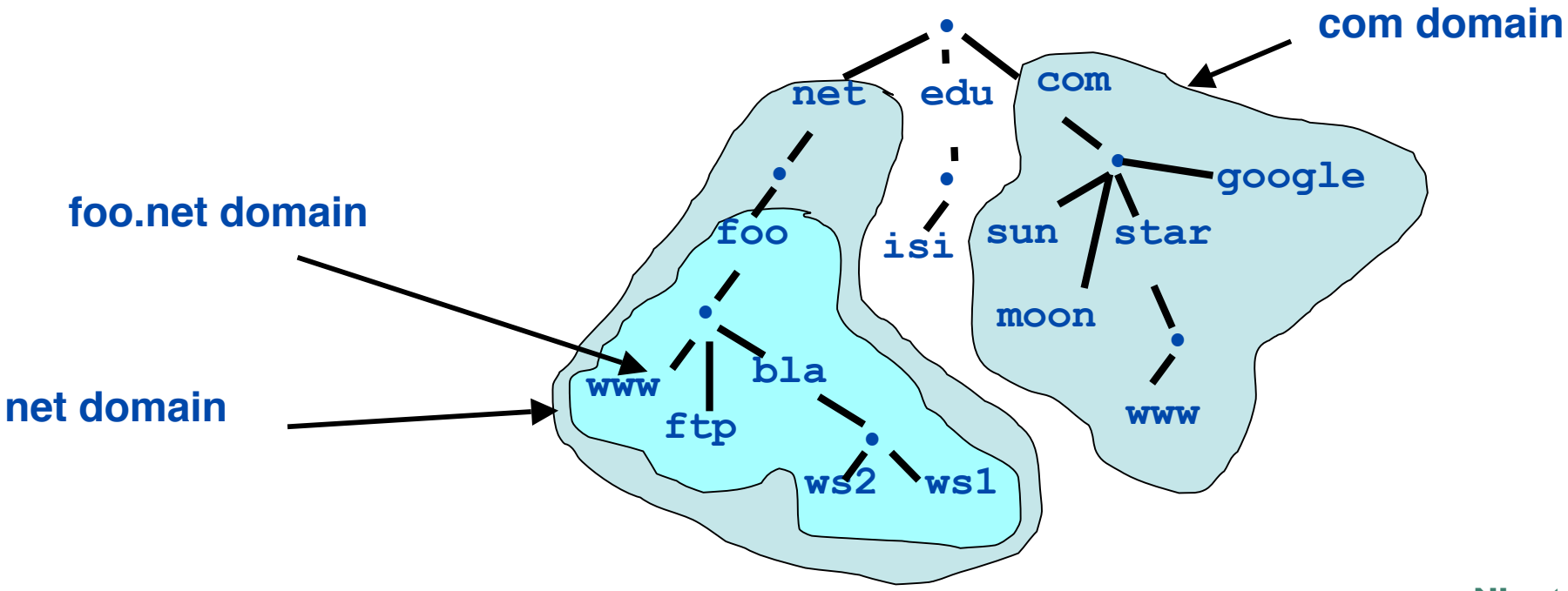
The Namespace Design

- The namespace needs to be made hierarchical to be able to scale
  - Both “technical” and “managerial” delegation
  - Control of parts of the namespace follows the hierarchy
  - Hierarchy represented in labels

    `player.testlab.nlnetlabs.nl`

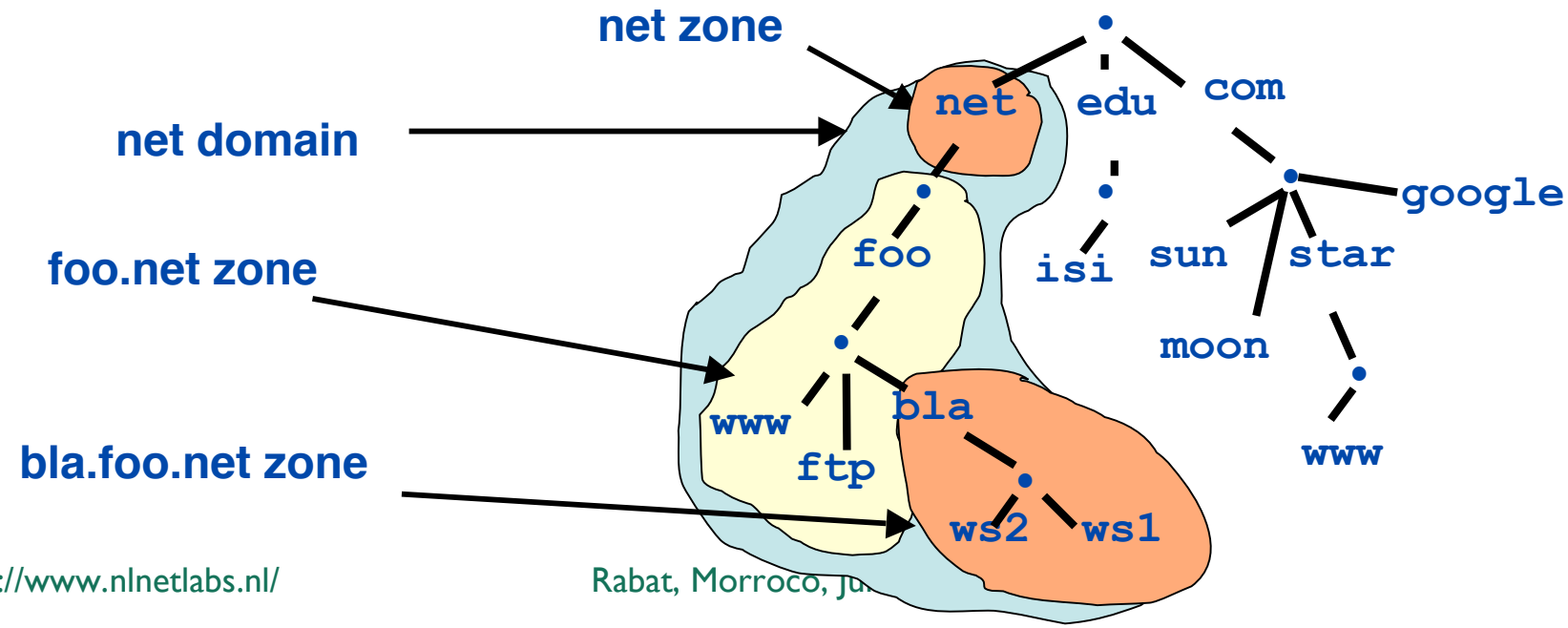
The namespace: Domains

- Domains are "namespace subsets"
- Everything below .com is in the com domain.
- Everything below foo.net is in the foo.net domain and in the net domain.

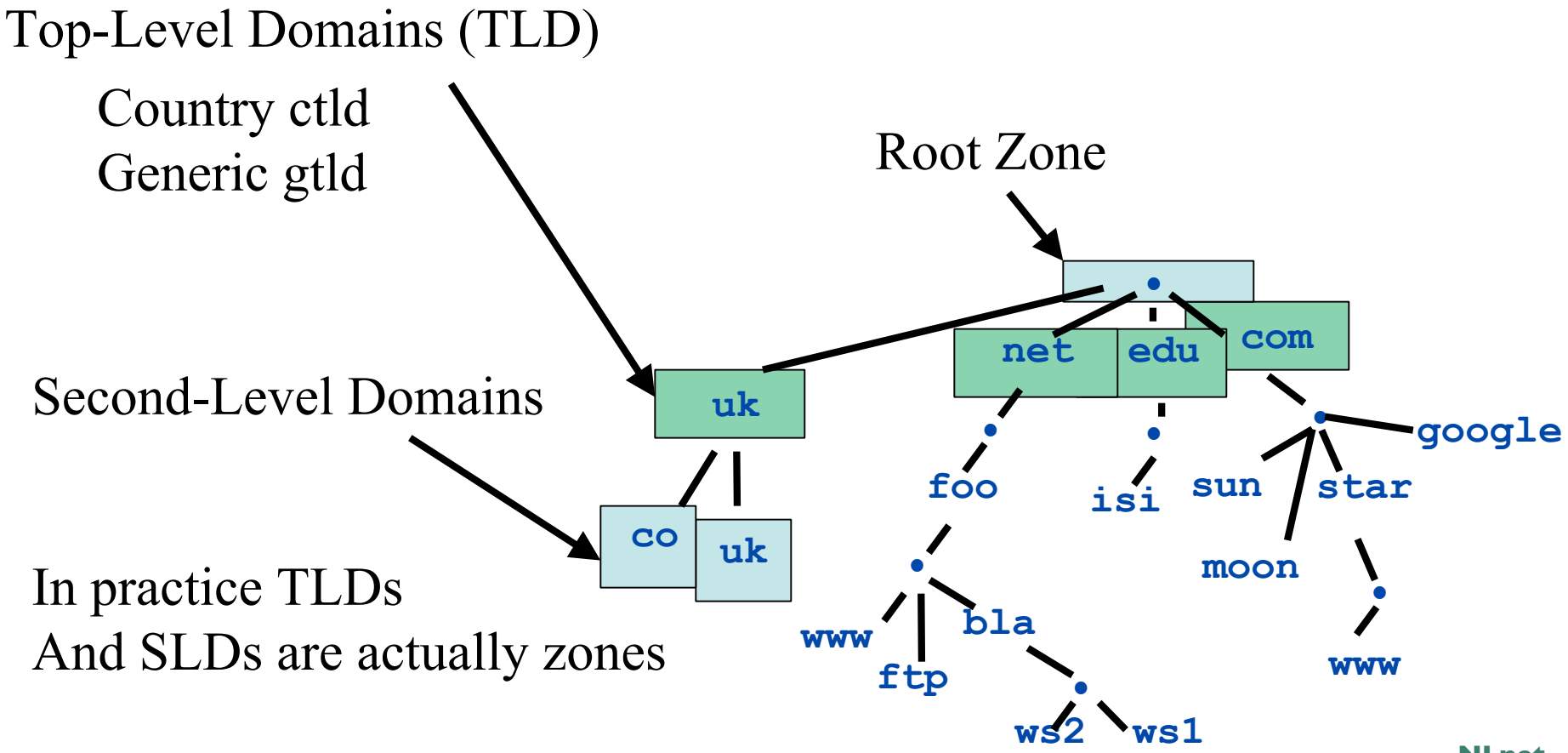


The namespace: Zones and Delegations

- 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



Some Jargon

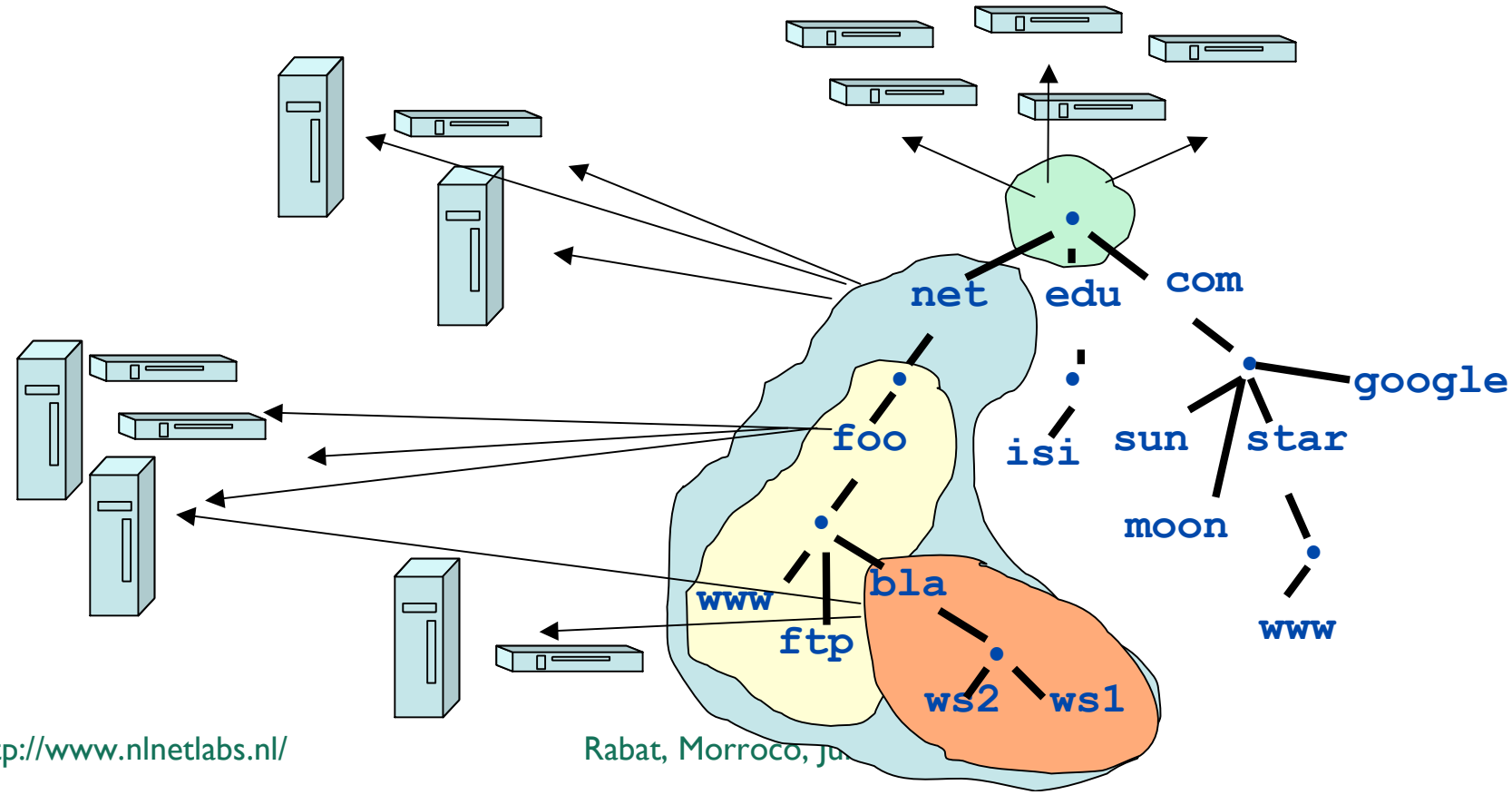

Top-Level Domains (TLD)
Country ctld
Generic gtld
Root Zone
Second-Level Domains
In practice TLDs
And SLDs are actually zones
uk
net
edu
com
co
uk
foo
isi
sun
star
google
moon
www
bla
www
ftp
ws2
ws1

Name Servers

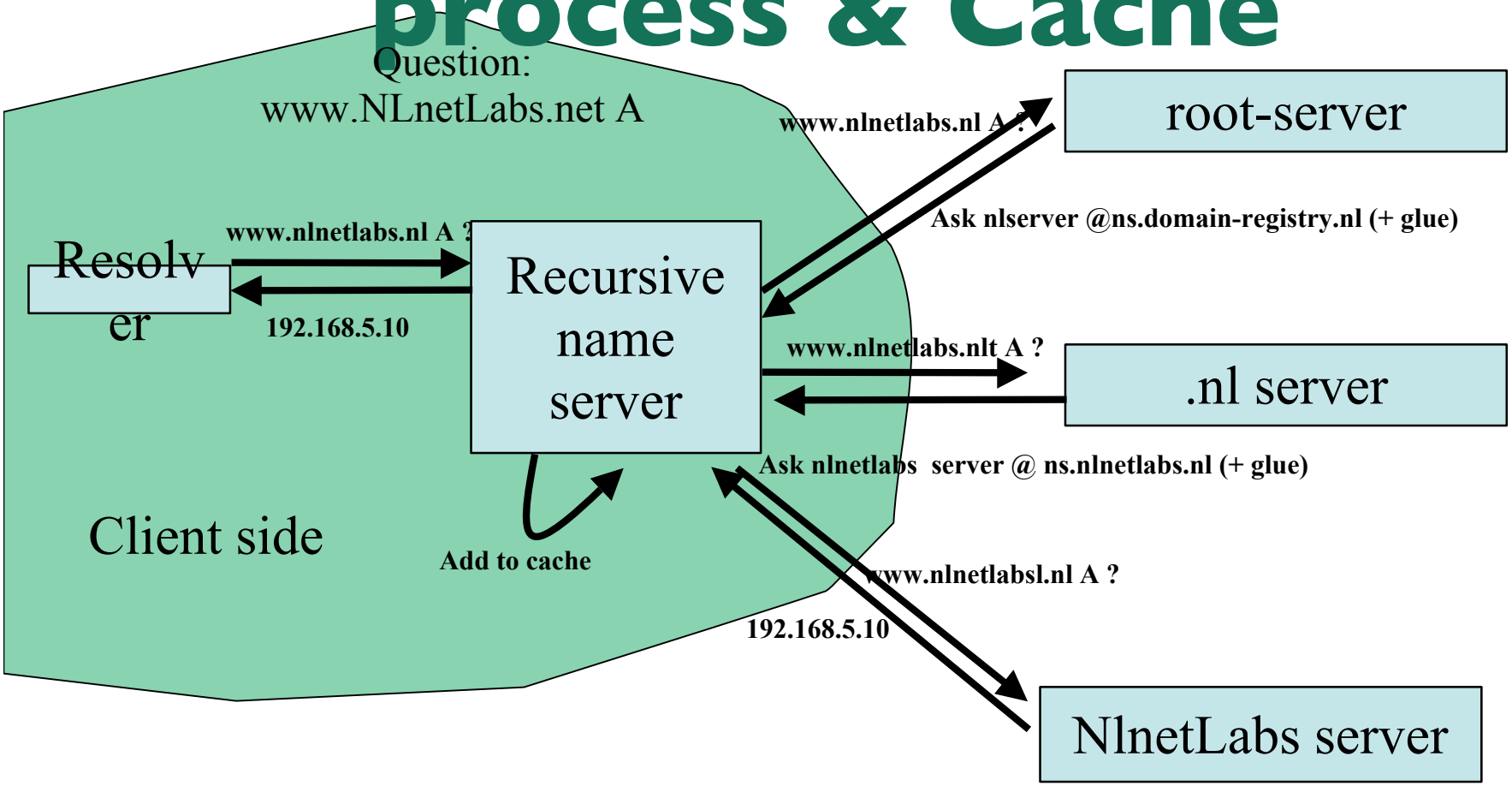
- Name servers answer 'DNS' questions.
- Several types of name servers
  - Authoritative servers
    - Serves the authoritative data for 'Zones'
    - Primary and Secondary
  - (Caching) recursive servers
    - Also called caching forwarders
  - Mixture of functionality

Zones are served by authoritative name servers

Each zone served by multiple servers (over 10^6) in total

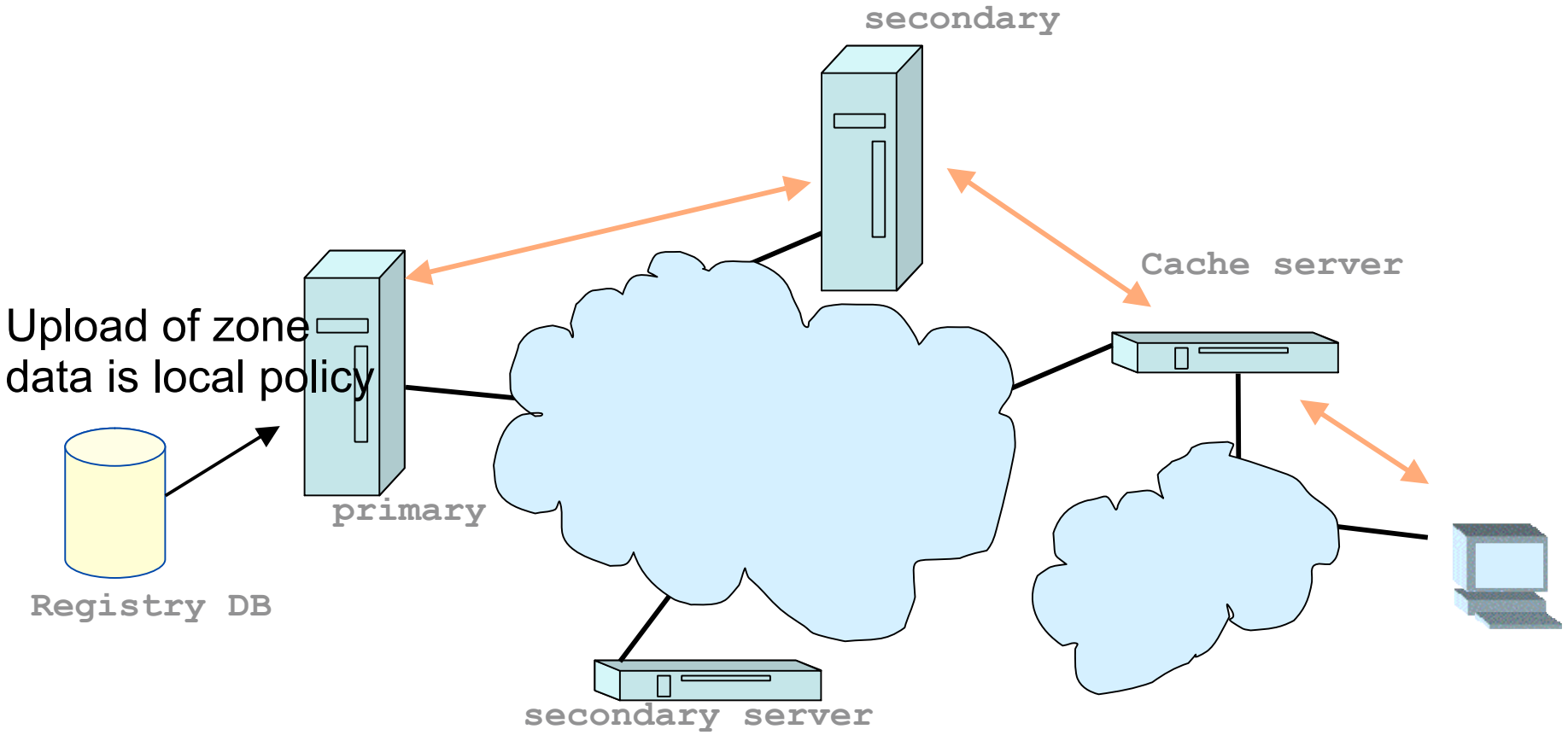


Concept: Resolving process & Cache



Hooking this together

Changes in DNS do not propagate instantly!



Presentation Road Map

- Why a naming system
- DNS Components
- DNS Features
- Techie details

DNS Features

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

DNS Features: Global Distribution

- Data is maintained locally, but retrievable globally
  - No single computer has all DNS data
  - Total number of servers: in the 10^6 to 10^7 range
- 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
- Response the same regardless of who the source of the query

DNS Features: Scalability

- No limit to the size of the database
  - One server has over 40,000,000 names
- No limit to the number of queries
  - 24,000 queries per second handled easily by one server
- Queries distributed among primaries, secondaries, and caches

DNS Features: Reliability

- Data is replicated
  - Data from primary is copied to multiple secondaries
  - The system can deal with outage of servers
- Clients can query
  - All authoritative servers
  - No difference between primaries and secondaries
- Clients will typically query local caches
- DNS protocols can use either UDP or TCP
  - If UDP, DNS protocol handles retransmission, sequencing, etc.

DNS Features: Dynamicity

- Database can be updated dynamically
  - Add/delete/modify of any record
  - Within seconds possible, traditionally lower update rates
- Modification of the primary database triggers replication
  - Only primary can be dynamically updated

Presentation Road Map

- Why a naming system
- DNS Components
- DNS Features
- Techie Details

RRs and RRSets

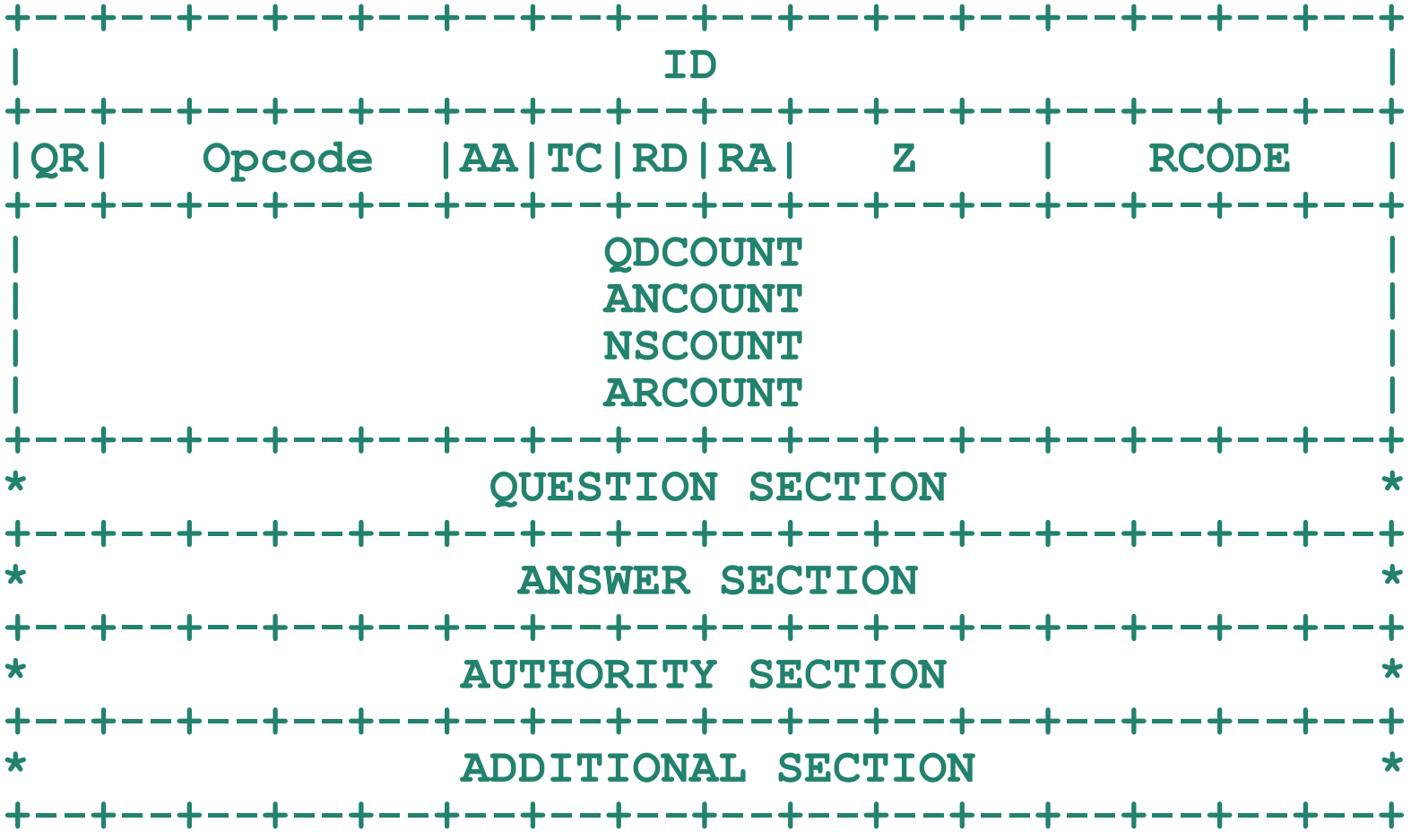
- Resource Record:
  - name TTL class type rdata

```
www.nlnetlabs.nl. 7200   IN  A   192.168.10.3
```

- RRset: RRs with same name, class and type:

```
www.nlnetlabs.nl. 7200 IN A  192.168.10.3
                       A  10.0.0.3
                       A  172.25.215.2
```

DNS Packet


ID
QR
Opcode
AA
TC
RD
RA
Z
RCODE
QDCOUNT
ANCOUNT
NSCOUNT
ARCOUNT
QUESTION SECTION
ANSWER SECTION
AUTHORITY SECTION
ADDITIONAL SECTION

DIG and the Packet

```
; <<>> DiG 9.3.2 <<>> www.nlnetlabs.nl
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50529
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.nlnetlabs.nl.      IN A

;; ANSWER SECTION:
www.nlnetlabs.nl.      86400 IN A 213.154.224.1

;; AUTHORITY SECTION:
nlnetlabs.nl.          78254 IN NS ns7.domain-registry.nl.
nlnetlabs.nl.          78254 IN NS open.nlnetlabs.nl.
nlnetlabs.nl.          78254 IN NS omval.tednet.nl.

;; ADDITIONAL SECTION:
open.nlnetlabs.nl.     78254 IN A 213.154.224.1
open.nlnetlabs.nl.     78254 IN AAAA 2001:7b8:206:1::53
open.nlnetlabs.nl.     78254 IN AAAA 2001:7b8:206:1:211:2fff:fed7:7378

;; Query time: 49 msec
;; SERVER: 172.16.16.1#53(172.16.16.1)
;; WHEN: Wed Oct  4 21:21:24 2006
;; MSG SIZE  rcvd: 202
```

QUESTIONS?
(Acknowledgements)

- A number of these slides are based on earlier work at RIPE NCC and course material developed for ISOC and APRICOT DNS courses.
  - Bill Manning and Ed Lewis co-authored the APRICOT DNS course.
  - Apologies for not mentioning other less significant sources