Domain Name System

Network Infrastructures labs

Marco Spaziani Brunella

SAPIENZA
UNIVERSITÀ DI ROMA

Lecture details

- **Readings:**
  - DNS and BIND; Paul Albitz; O'Reilly Media
- **Lecture outline:**
  - DNS Theory
  - BIND

Need for name translation

- initially because tty2 is better than port 21
- ...imagine IPV6!
  - 2002:a050:6768:0:e2f8:47ff:fe38:c5cc: (my pc)
- Important also for:
  - load balancing
  - decoupling IP and name (i.e. when changing hosting)
  - many other things (e.g. anti-spam!)

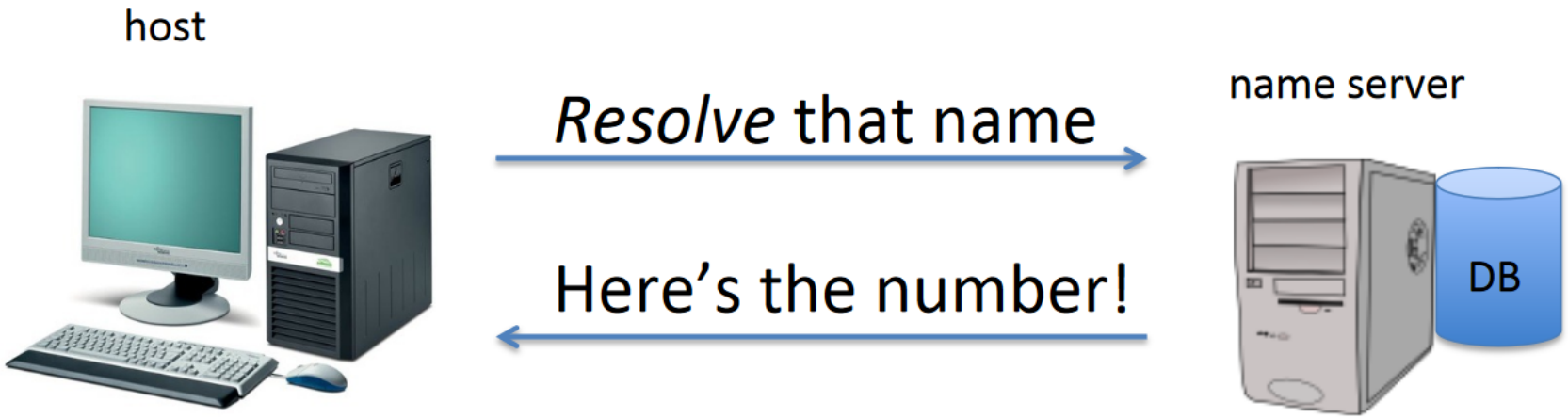
Before DNS

- Each computer has HOSTS.txt
  - still used in all operating system, check your one!

```
127.0.0.1 localhost
```

- Try to put in /etc/hosts:
  - 63.135.91.11 facebook.com
- Inefficiencies: traffic load, name collisions, consistencies

Simple solution



On Internet

- need of a *scalable* solution (today > ~284M domains[1])
- avoid name collision
- reliability
- introduce hierarchical names: *www.example.com.*
- Key concept: *authority and delegation*

"silent dot"

[1] https://investor.verisign.com/releasedetail.cfm?releaseid=892548

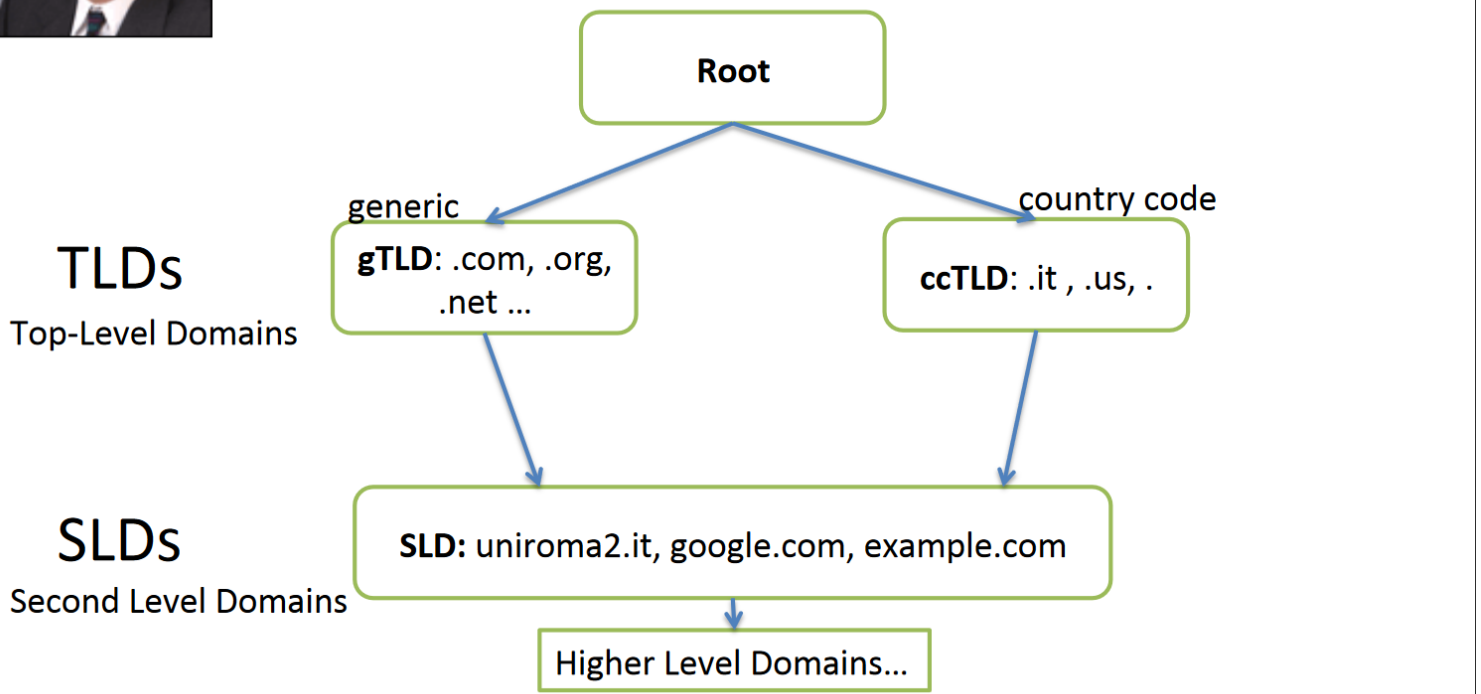
Internet domain name system 1/2

- DNS's distributed database is indexed by domain names
- Each domain name is essentially just a path in a large inverted tree, called the *domain name space*
- Each node in the tree has a text label (without dots) that can be up to 63 characters long
- The full *domain name* of any node in the tree is the sequence of labels on the path from that node to the root
- An absolute domain name is also referred to as a *fully qualified domain name*, often abbreviated *FQDN*
- DNS requires that sibling nodes – nodes that are children of the same parent – have different labels. This restriction guarantees that a domain name uniquely identifies a single node in the tree (easier collision avoidance)
- Scalability is reached through DELEGATION

Internet domain name system 2/2

First experiment by Paul Mockapetris 1983

Internet Domain Name System



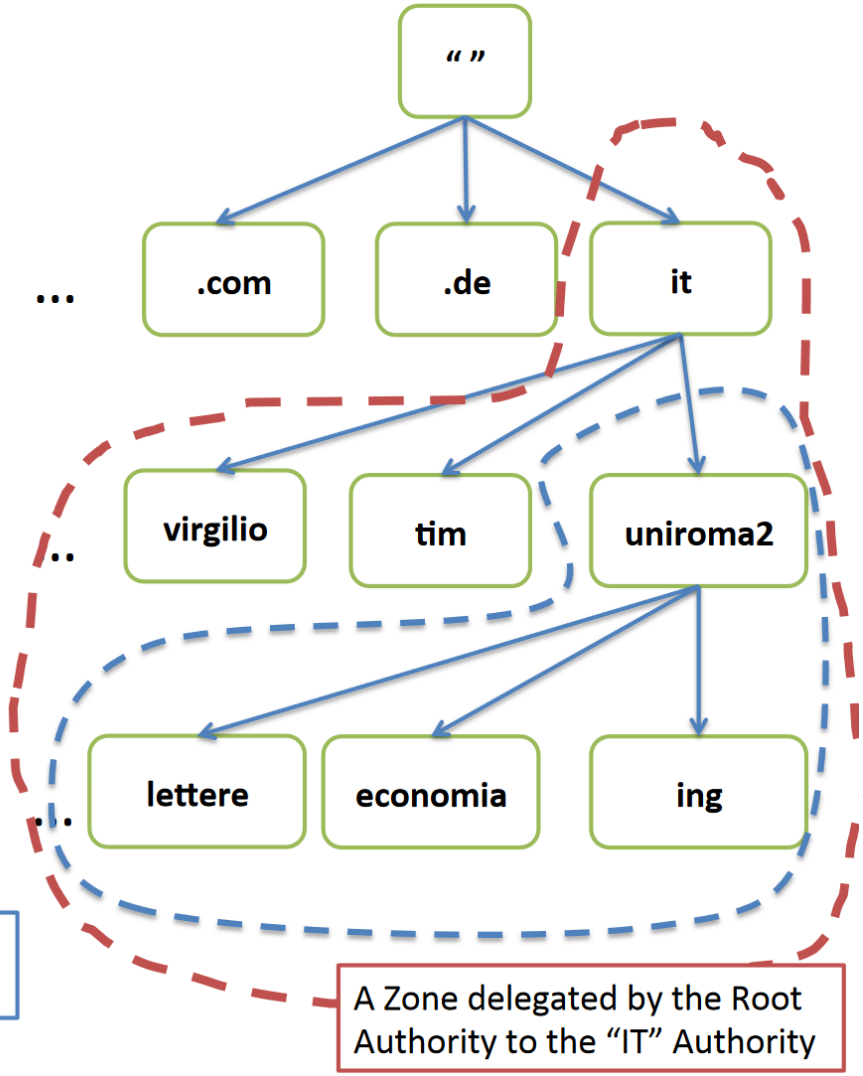
A **Domain** is a string representing the realm of an **Authority**

for root: IANA (departement of ICANN—www.icann.org/)

for .it: is @ Istituto per le Applicazioni Telematiche del CNR, PISA.

DNS Tree

- The administrative responsibility of part of the Domain Name Space can be delegated: this is called a zone
- The zone can sub-delegate
- Zone are represented using zone files (RFC 1034-1035)



Resource Records

- Every of the tree could have some Resource Records that contain information about the domain name
  - RR have different *standardized* types (e.g. A, PTR, MX)
  - For instance, the IPv4 Address associated with a name (Resource Record of type A)

Registrar, Registry, Maintainer

- **Registry**: database of all domain names registered in a top-level domain or second-level domain extension
- **Registrar**: frontend to the public
  - accredited by a gTLD or ccTLD:
    - Example http://www.nic.it/cgi-bin/List/index.cgi
  - Works with "web pages" (*asynchronous*)
- **Maintainer**: frontend to the public
  - accredited by a gTLD or ccTLD
  - Works with FAX (*synchronous*) **OBSOLETE***

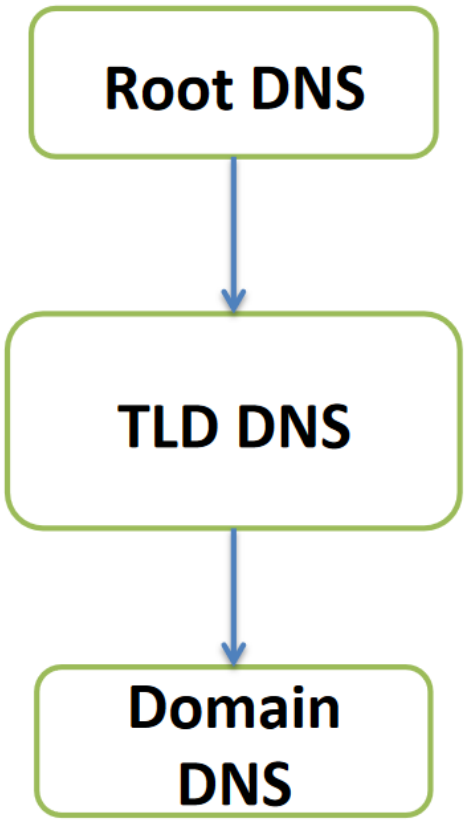
* From 1 July 2010 no more maintainer contracts for .it domains (source: registro.it)

www.example.com

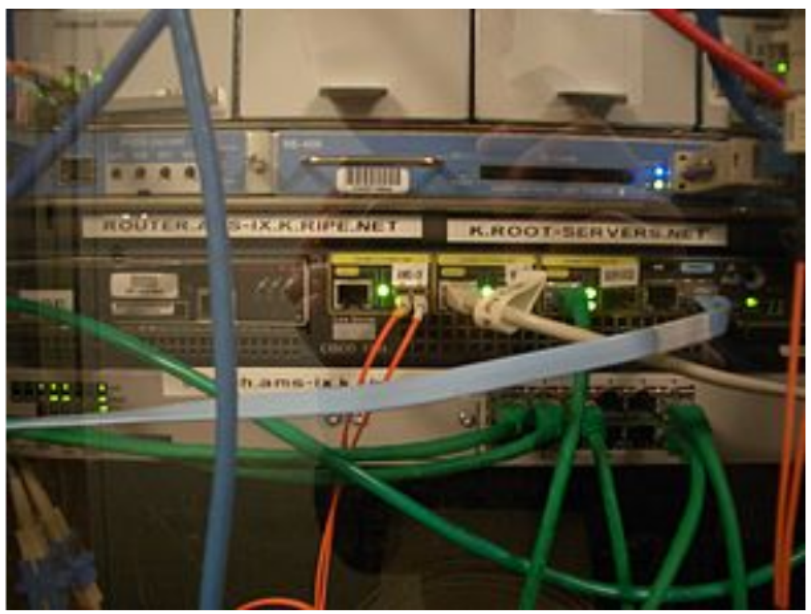
- The domain name example.com was delegated from a **gTLD authority**, which in turn was delegated from **ICANN** (authority for DNS Root Zone)
- The owner of the domain chooses the www part (called host name)
- This is a Fully Qualified Domain Name (**FQDN**)
  - specifies an exact location in the DNS tree hierarchy

DNS Implementation

- Exactly maps the domain name delegation structure



13 root-servers
(from a.root-servers.net to m)



DNS Recipe

1. Zone files
   - translates the domain names into operational entities, such as hosts, mail servers, services for use by DNS software.
   - standard with Resource Records (RFC 1035, so portable!)
2. DNS program
3. Resolver library (ask the questions)

Iterative DNS Queries

Query www.uniroma2.it →

root server

← referral to .it ccTLD DNS

Query www.uniroma2.it →

TLD DNS

← referral to uniroma2.it DNS

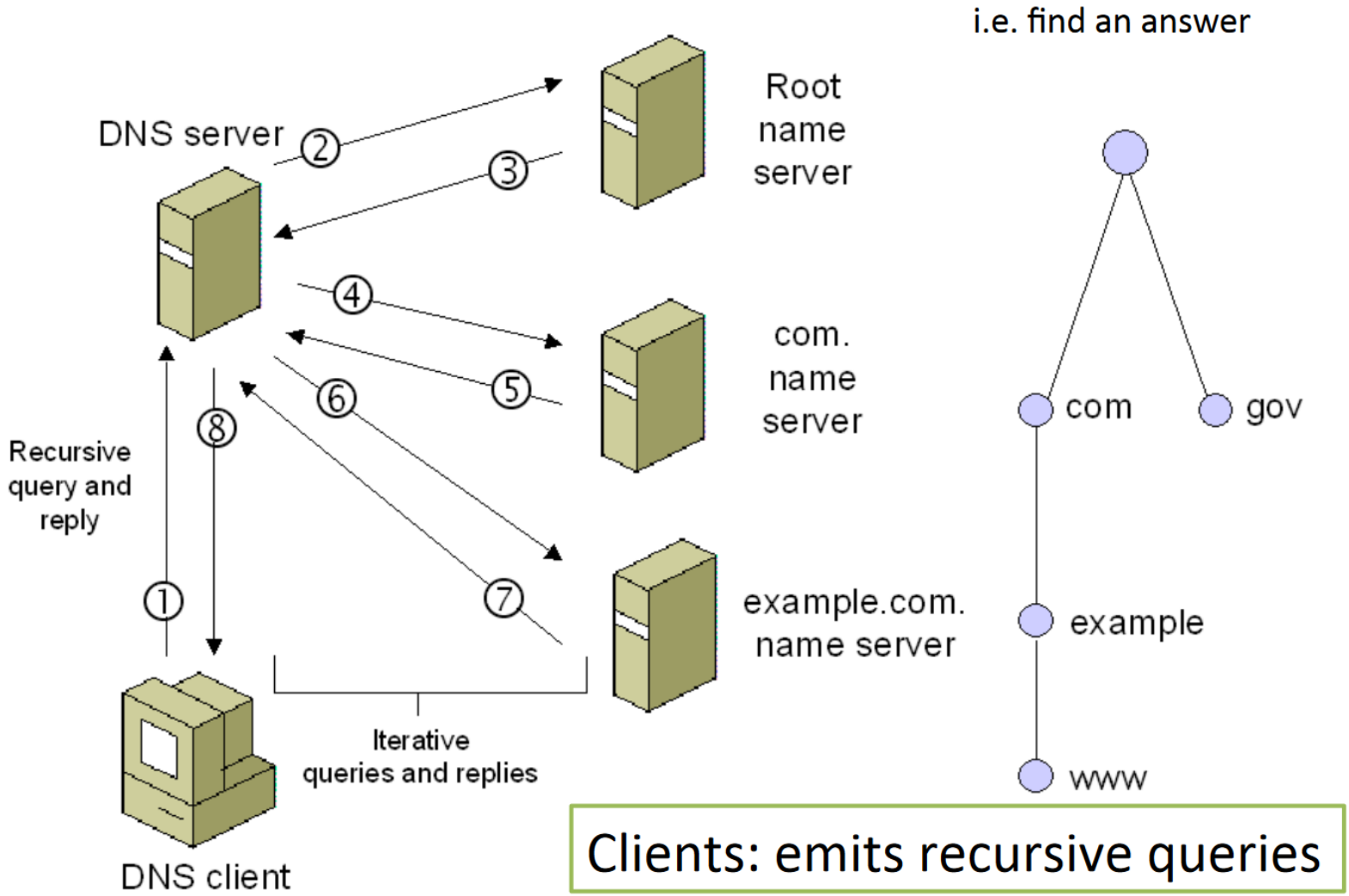
Query www.uniroma2.it →

Domain DNS

← Authoritative answer

Root Servers: response to only iterative queries

Recursive DNS Queries



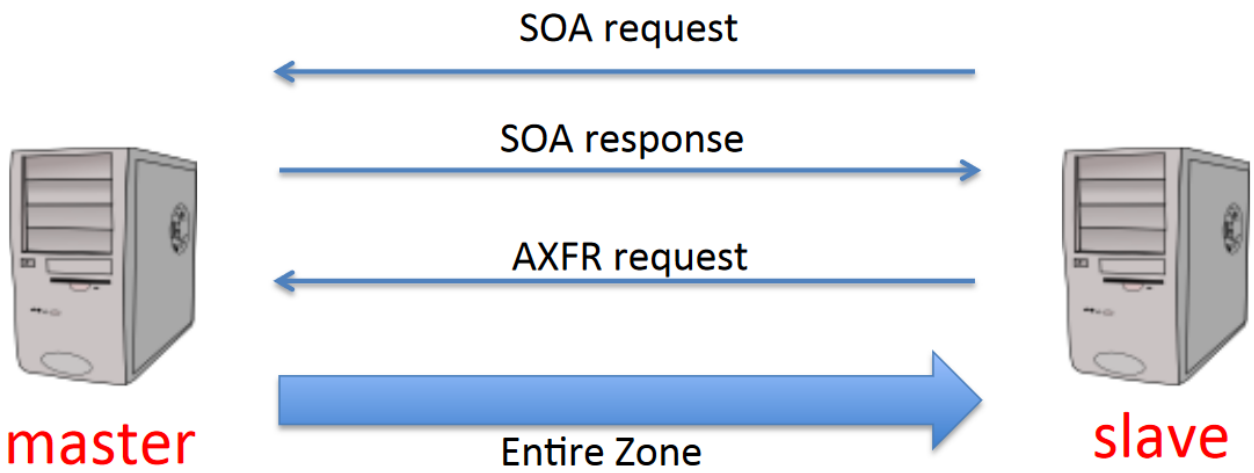
i.e. find an answer

Clients: emits recursive queries

DNS Resolver

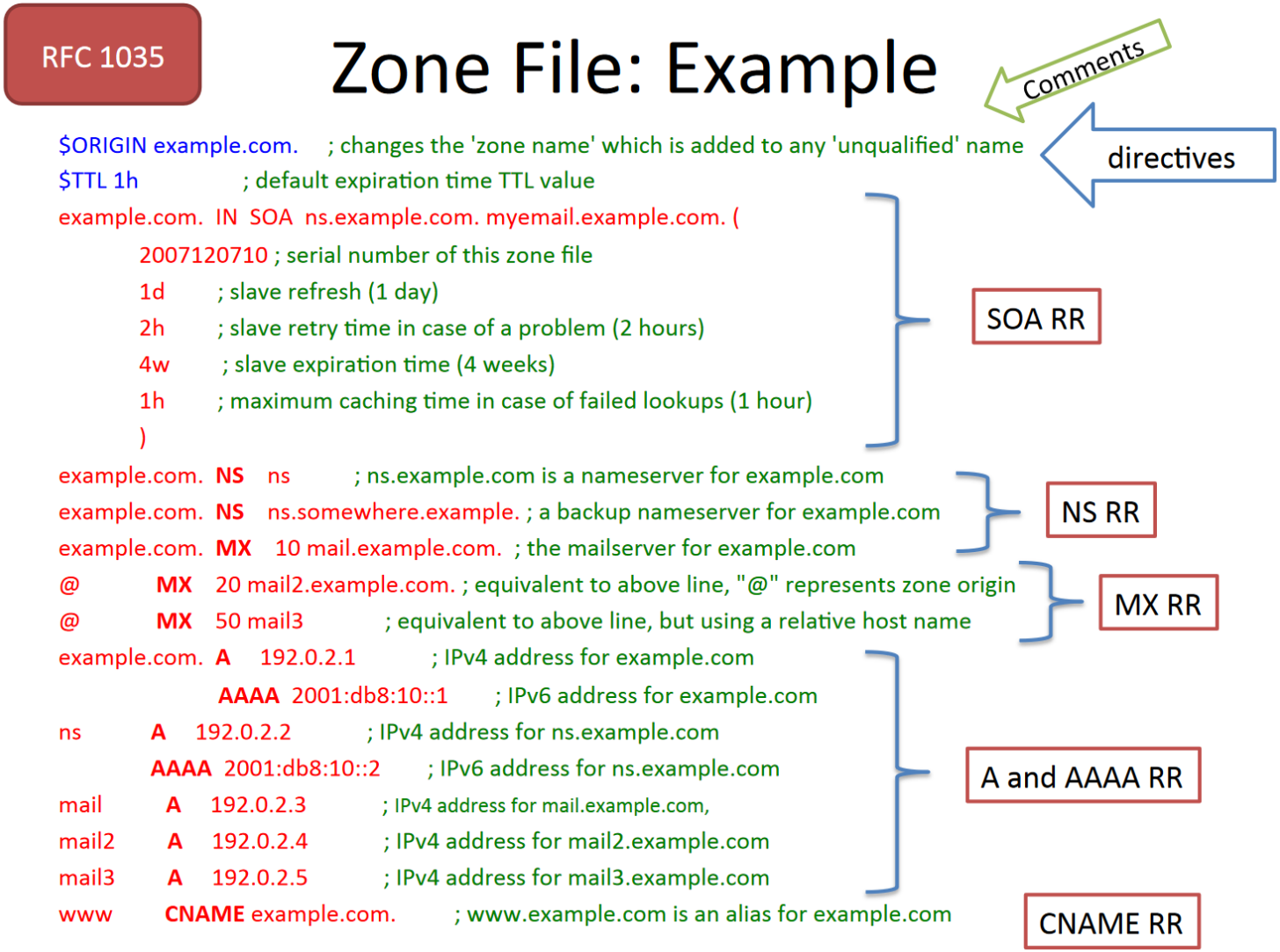
- The client-side of the DNS is usually called a DNS resolver.
- On PC, we usually have simple resolvers (called "stub resolvers") that can not follow referrals
  - Need a recursive DNS
- Browser use *gethostbyname* or *gethostbyaddr* methods to invoke name/ip resolution
  - functions provided by the stub resolver

Master-Slave configuration



- redundancy for load balancing and fault resilience
- zones are passed from master to slave
  - full or partial zone transfer
- timing?

Zone file


RFC 1035
Zone File: Example
Comments
directives
$ORIGIN example.com. ; changes the 'zone name' which is added to any 'unqualified' name
$TTL 1h ; default expiration time TTL value
example.com. IN SOA ns.example.com. myemail.example.com. (
2007120710 ; serial number of this zone file
1d ; slave refresh (1 day)
2h ; slave retry time in case of a problem (2 hours)
4w ; slave expiration time (4 weeks)
1h ; maximum caching time in case of failed lookups (1 hour)
)
SOA RR
example.com. NS ns ; ns.example.com is a nameserver for example.com
example.com. NS ns.somewhere.example. ; a backup nameserver for example.com
NS RR
example.com. MX 10 mail.example.com. ; the mailserver for example.com
@ MX 20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@ MX 50 mail3 ; equivalent to above line, but using a relative host name
MX RR
example.com. A 192.0.2.1 ; IPv4 address for example.com
AAAA 2001:db8:10::1 ; IPv6 address for example.com
ns A 192.0.2.2 ; IPv4 address for ns.example.com
AAAA 2001:db8:10::2 ; IPv6 address for ns.example.com
mail A 192.0.2.3 ; IPv4 address for mail.example.com,
mail2 A 192.0.2.4 ; IPv4 address for mail2.example.com
mail3 A 192.0.2.5 ; IPv4 address for mail3.example.com
A and AAAA RR
www CNAME example.com. ; www.example.com is an alias for example.com
CNAME RR

Resource Records: SOA

- A Start of Authority (SOA) RR :
  - describes global characteristics of the zone domain
  - one and only one for each zone file (first RR in a zone file)
- Name Server (NS) RR: Defines name servers that are authoritative for the zone or domain. There must be two or more NS Resource Records in a zone file. NS RRs may reference servers in this domain or in a foreign or external domain. These RRs are mandatory.
- Mail Exchanger (MX) RR: Defines the mail servers for the zone (optional)
- Address (A) RR: Define the IPv4 address of all the hosts (or services) that exist in this zone and which are required to be publicly visible. IPv6 entries are defined using AAAA (called Quad A) RRs (optional)
- Canonical Name (CNAME) RR: Defines an Alias RR, which allows one host (or service) be defined as the alias name for another host (optional)
- And: PTR, TXT, AAAA, SRV and NSEC, RRSIG, DS, DNSKEY, KEY (DNSSEC)

SOA Syntax

- Specifies authoritative information about a DNS zone

Zone Domain	Class	RR	NS	email dnsmaster
example.com.	IN	SOA	ns.example.com.	email.example.com.

- Several parameters
  - serial: date (convention: YYYYMMDDSS)
  - refresh: tell to slave how often check for changes (default 3600)
  - retry: interval between two subsequent attempt to contact the master in case of problems (default 600)
  - expire: if slave fails to contact master after expire time, it stops to resolve that zone (default 86400)
  - ttl The minimum time-to-live value applies to all resource records in the zone file (default 3600)

NS Syntax

- Delegates a DNS zone to use the given authoritative name servers

Zone Name	TTL	class	rr	dns name
example.com.		IN	NS	ns1.example.com.

- The name field can be any of:
  - A Fully Qualified Domain Name (FQDN) e.g. example.com. (ends with a dot)
  - An unqualified name (does not end with a dot)
  - An '@' (substitutes the current value of $ORIGIN)
  - a 'space' or 'blank' (tab) - this is replaced with the previous value of the name field. If no name has been previously defined this may result in the value of $ORIGIN.

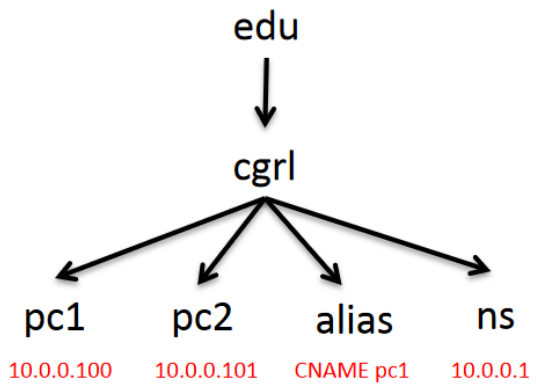
A Syntax

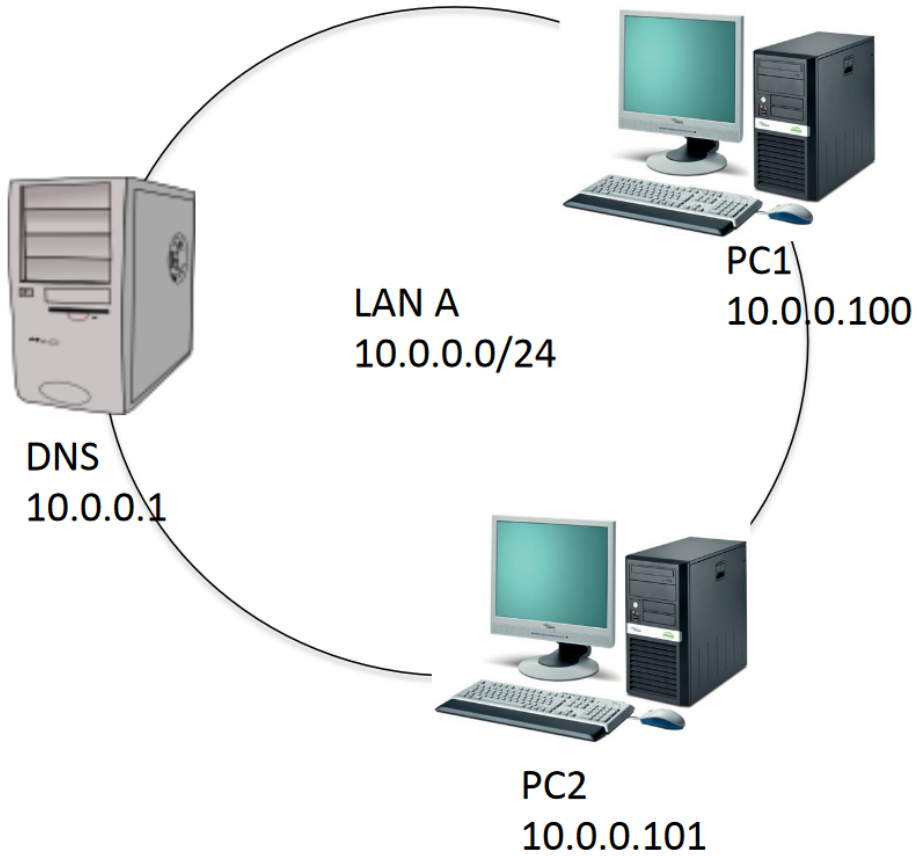
- Resolve a name to a IPv4 address

Name	TTL	class	rr	Address
example.com.		IN	A	93.184.216.119

lab_dns_0

DNS (ns.cgrl.edu.) is the authoritative name server for the zone cgrl.edu.





BIND

- bind executable: /usr/sbin/named
- rndc: command line administration of the named daemon
- Like many daemons got its start/stop script in /etc/init.d
  - /etc/init.d/bind [start stop restart status reload]
- Good news! Only one (usually short) conf file: /etc/bind/named.conf
- Bad news! it includes several other files!! such as:
    - Zone files: in /etc/bind/. Example: db.edu.cgrl
    - options: /etc/bind/named.conf.options
    - other files

/etc/bind/named.conf

```
zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

include "/etc/bind/named.conf.local";
```

FIRST STEP: Add a zone for cgrl.edu to /etc/bind/db.edu.cgrl

Configuration files

/etc/bind/named.conf

```
zone "cgrl.edu" {
        type master;
        file "/etc/bind/db.cgrl.edu";
};
```

/etc/bind/db.edu.cgrl

```
$TTL 2d
cgrl.edu. IN SOA ns.cgrl.edu. hostmaster.cgrl.edu. (
    2014050600 ; serial
    28 ; refresh
    14 ; retry
    3600000 ; expire
    0 ; negative cache ttl
)

cgrl.edu.   IN      NS      ns.cgrl.edu.

alias.cgrl.edu. IN      CNAME   pc1.cgrl.edu.

ns.cgrl.edu.        IN      A       10.0.0.1
pc1.cgrl.edu.       IN      A       10.0.0.100
pc2.cgrl.edu.       IN      A       10.0.0.101
```

Check configuration files

- To check zone files:
  - named-checkzone $ZONE_NAME $ZONE_FILE
- To check conf files:
  - named-checkconf
- View in syslog (or, if in another log file if you changed it)

```
dns:~# named-checkconf
dns:~# named-checkzone cgrl.edu /etc/bind/db.cgrl.edu
zone cgrl.edu/IN: loaded serial 2012032200
OK
dns:~#
```

/etc/resolv.conf

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

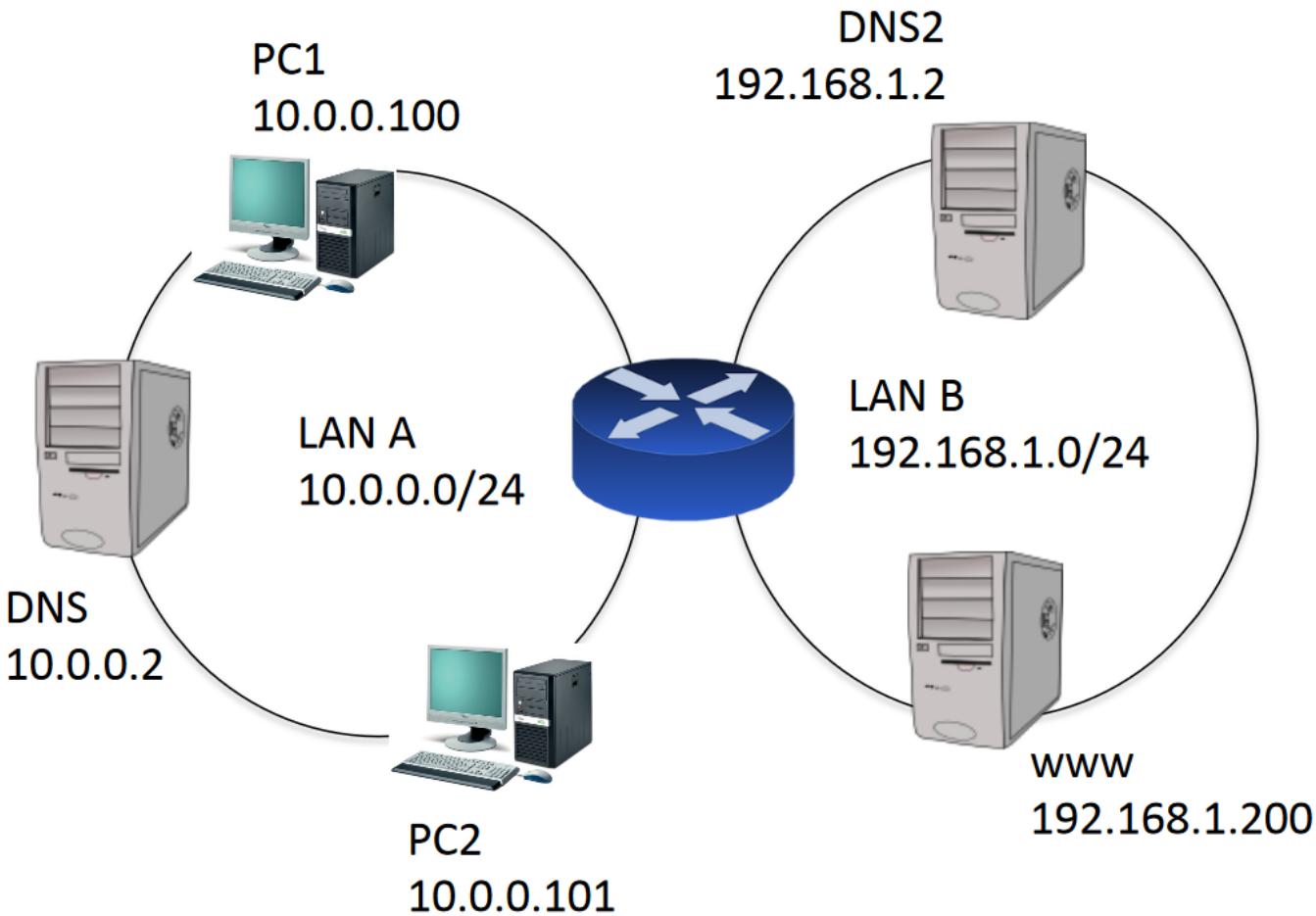
primary DNS
secondary DNS

```
domain mydomain.com
search mysearch.com d2.com
```

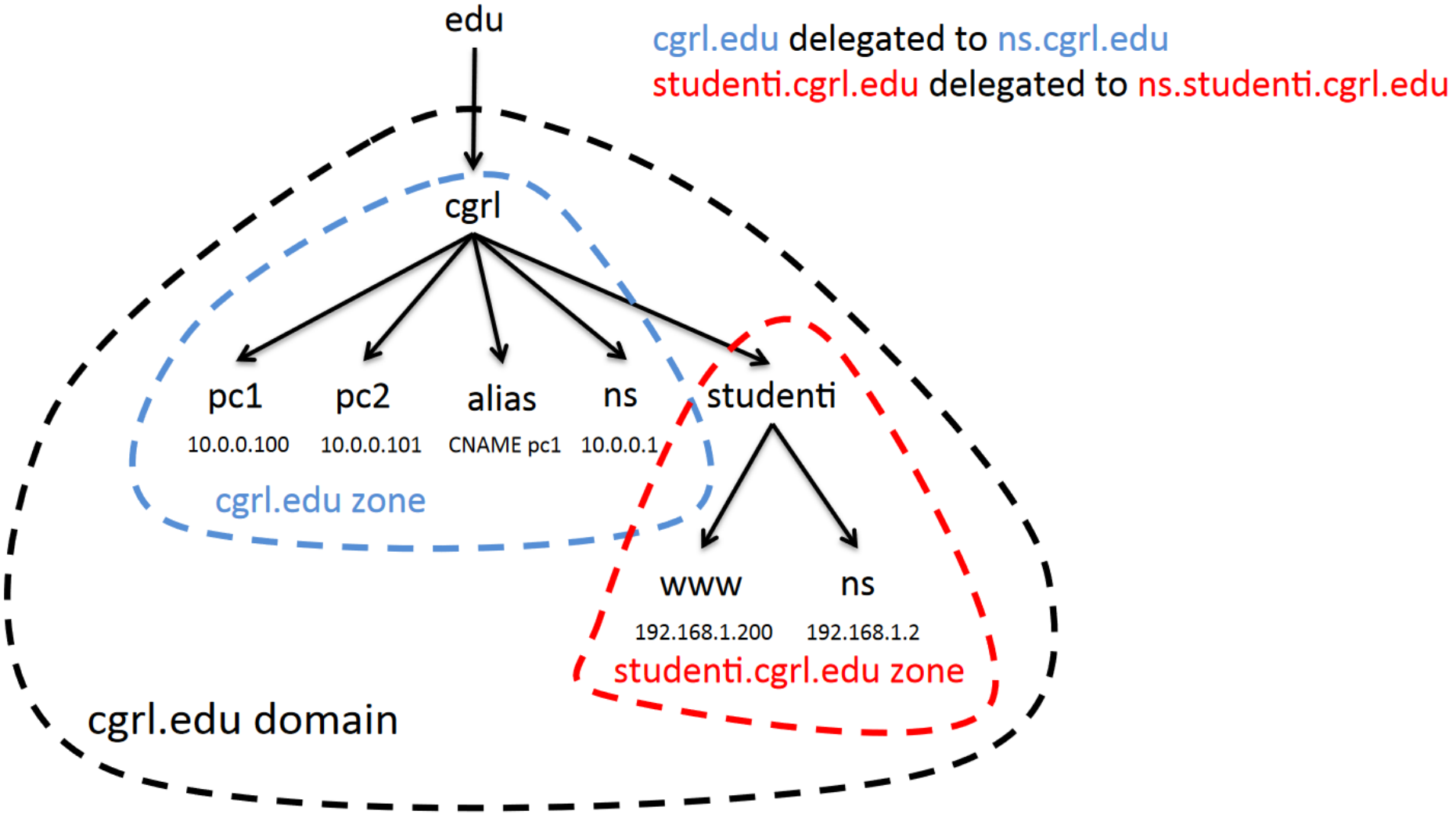
search directive for short names

- When try to resolv “test” it resolve test.mydomain.com (using **gethostname** or *domain* if present)
- If you want that test will be resolved as test.A and test.B specify search A B. (in case test.A fails, resolver will go for test.B)
- The **domain** and **search** keywords are mutually exclusive. If more than one instance of these keywords is present, the last instance wins.
- *Let’s put 127.0.0.1 to test our new dns server!!*

lab_dns_1


PC1
10.0.0.100
DNS2
192.168.1.2
LAN A
10.0.0.0/24
LAN B
192.168.1.0/24
DNS
10.0.0.2
PC2
10.0.0.101
www
192.168.1.200

Delegation scheme



Delegation configuration

dns#/etc/bind/db.edu.cgrl

```
$ORIGIN cgrl.edu.
$TTL 2d
@ IN SOA ns.cgrl.edu. hostmaster.cgrl.edu. (
    2012032200 ; serial
    28 ; refresh
    14 ; retry
    3600000 ; expire
    0 ; negative cache ttl
)

@           IN      NS      ns
ns          IN      A       10.0.0.2
pc1         IN      A       10.0.0.100
pc2         IN      A       10.0.0.101

$ORIGIN studenti.cgrl.edu.
@           IN      NS      ns.studenti.cgrl.edu.
ns          IN      A       192.168.1.2
```

@ substitutes the current value of $ORIGIN

Relative names appended to current zone

delegation

Glue Record

- How we can resolve ns.studenti.cgrl.edu?
  - if that was exactly the dns responsible to resolve *.studenti.cgrl.edu!!
- A glue record is an A record for the name server that is authoritative for the delegated zone
  - ns.studenti.cgrl.edu IN A 192.168.1.2

Delegated configuration

Add to dns2#/etc/bind/named.conf

```
zone "studenti.cgrl.edu" {
        type master;
        file "/etc/bind/db.studenti.cgrl.edu";
};
```

dns2#/etc/bind/db.studenti.cgrl.edu

```
$ORIGIN studenti.cgrl.edu.
$TTL 2d
@ IN SOA ns.studenti.cgrl.edu. hostmaster.studenti.cgrl.edu. (
    2012032200 ; serial
    28 ; refresh
    14 ; retry
    3600000 ; expire
    0 ; negative cache ttl
)

@           IN      NS      ns
ns          IN      A       192.168.1.2
www         IN      A       192.168.1.200
```