

*Corsi di reti  
per laurea triennale*

*Lezione 5  
DNS*

Claudio Covelli

Trento, 1 novembre 2006

---

---

# Agenda

## DNS

- Scopo
- Breve storia
- Filosofia realizzativa
- Meccanismi di delega
- Esempi

# DNS

## DNS (Domain Name System)

- Un client accede al server conoscendo 5 valori:
  - protocollo (TCP/UDP)
  - indirizzo IP mittente
  - porta (efemerale) mittente
  - indirizzo IP destinatario
  - porta destinatario
- Questi valori consentono di attivare la **socket di connessione client-server**
- I parametri protocollo, indirizzo IP mittente sono noti a priori; porta mittente viene determinata in modo automatico

# DNS

## DNS (Domain Name System)

- La porta del destinatario molte volte non deve essere specificata in quanto legata al protocollo utilizzato ([well-known ports](#))
- Spesso, al posto dell'indirizzo IP del server, è conosciuto, da chi utilizza il client, solo il suo [indirizzo mnemonico](#)

# DNS

## DNS (Domain Name System)

- Occorre quindi un meccanismo (**DNS**) che sia in grado di trasformare il nome mnemonico di un server in un indirizzo IP
- Il DNS (Domain Name System) è:
  - un insieme di nomi che consentano di individuare in modo univoco gli host di Internet
  - un insieme di server e di protocolli per la gestione e l'utilizzo di tali insiemi di nomi
- Lo scopo del DNS è la trasformazione di un nome mnemonico in indirizzo IP e viceversa (mapping)

Esempio: da [www.google.it](http://www.google.it) a 66.102.9.104 e viceversa

# DNS

## DNS: breve storia

- Inizialmente i client gestivano il mapping, memorizzando un file testuale (HOST.TXT) riportante, per ogni indirizzo IP, il relativo nome mnemonico
- La versione originale di tale file era detenuta presso l'Università di Stanford (SRI NIC) che gestiva tutti gli indirizzi IP mondiali
- Periodicamente ogni client scaricava, via FTP, tale file sul proprio hard disk in modo da aggiornare le definizioni
- Con il crescere di Internet, questo sistema si rivelò inefficace

# DNS

## DNS (Domain Name System): problemi di scalabilità

- **Banda:** il file host.txt assumeva di giorno in giorno dimensioni sempre maggiori e questo comportava elevato impegno di banda nel download
- **Univocità dei nomi:** SRI NIC assegnava gli indirizzi ma non aveva alcuna autorità sui nome. Ciò comportava potenziali problemi di duplicazione (clashing) con effetti ben evidenti
- **Inefficienza:** ogni giorno sempre più host si collegavano ad Internet ed il sistema basato sulla distribuzione di un singolo file non riusciva a garantire una rapida sincronizzazione

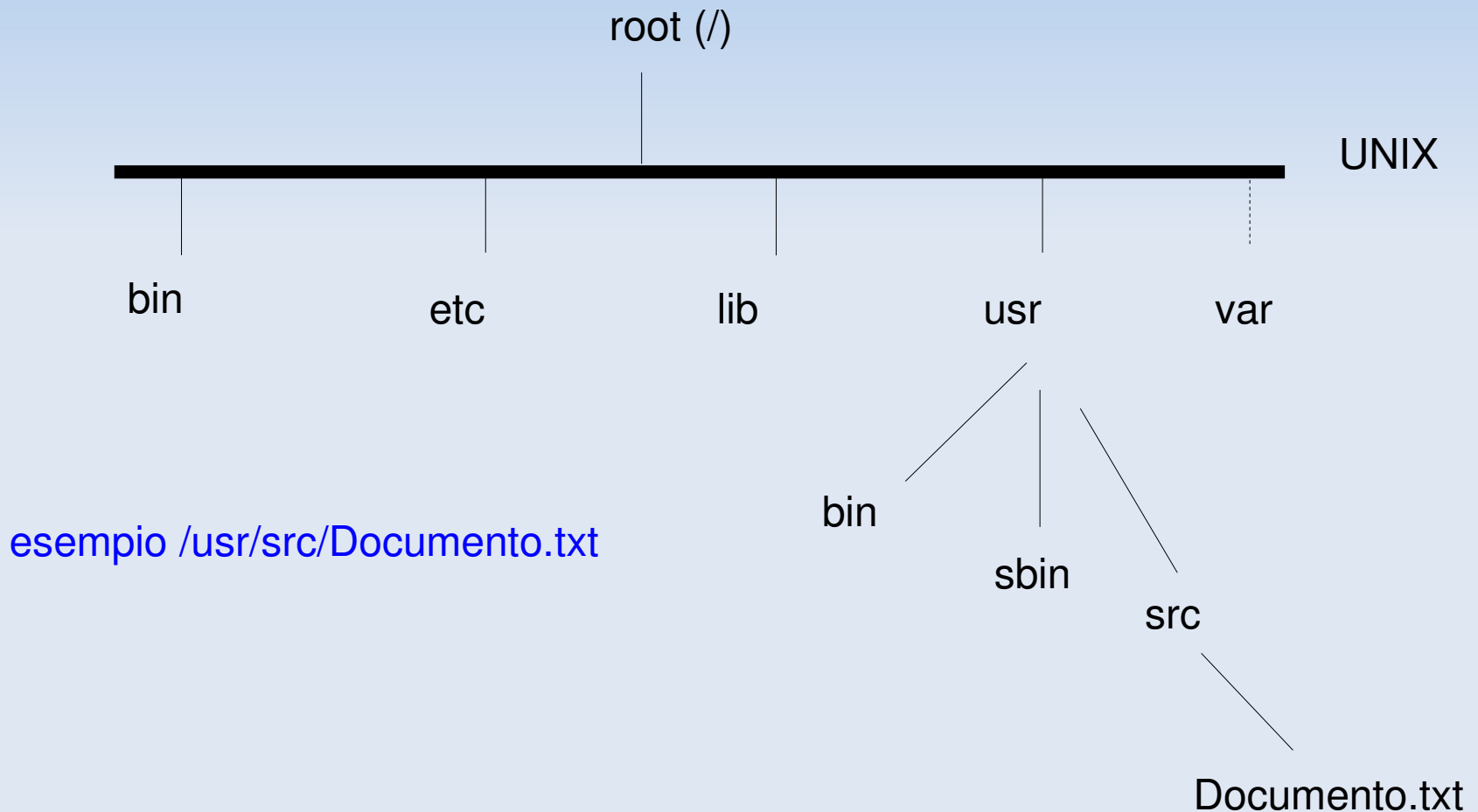
# DNS

## DNS (Domain Name System)

- Si progettò quindi una nuova architettura (DNS) che:
  - consentisse una gestione distribuita del mapping
  - ne garantisse, nel contempo, una visione integrata ed unitaria
- I nomi degli host appartenenti ad Internet vengono definiti, **in analogia ai nomi delle directory di un file system Unix**, mediante una struttura **ad albero rovesciato (inverted tree)** in cui:
  - la radice rappresenta il cosiddetto dominio di root (analogo alla root di un file system unix)
  - ogni nodo costituisce a sua volta la radice di un sottoalbero (subtree)
  - ogni subtree rappresenta un **dominio** (directory in Unix)
  - **ogni foglia rappresenta un host**

# DNS

## DNS (Domain Name System)

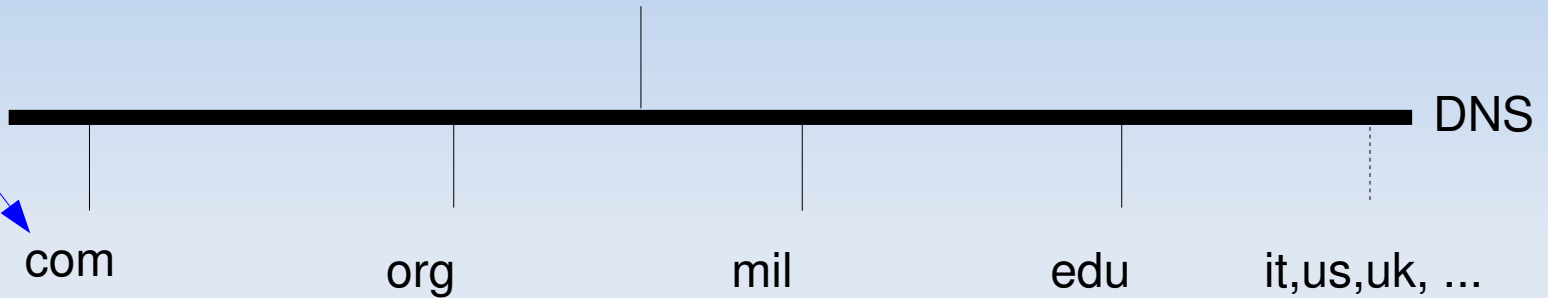


# DNS

## DNS (Domain Name System)

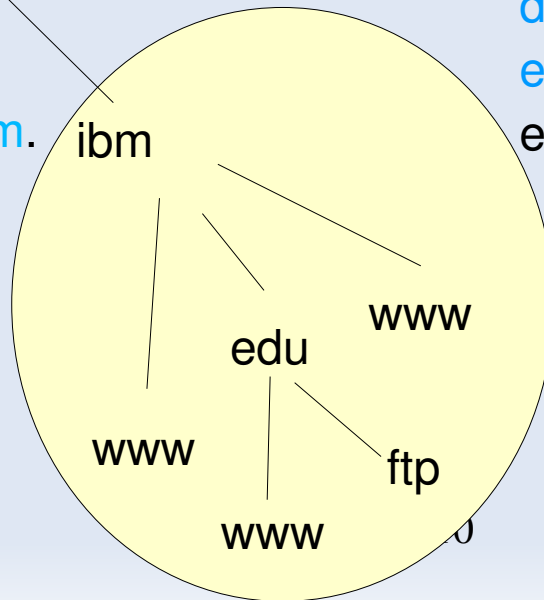
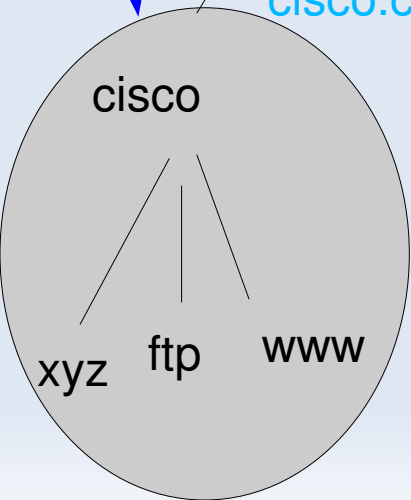
nodo =  
dominio

root (si indica con spazio vuoto)



dominio  
cisco.com.

dominio ibm.com.  
e sottodominio  
edu.ibm.com.



Fully Qualified Domain Name  
(FQDN)

host.dominio

Esempi (notare il punto)

www.ibm.com.

ftp.cisco.com.

# DNS

## DNS (Domain Name System)

- Ogni nodo ed ogni foglia hanno una label, analogamente ai files ed alle directories di Unix
- Il nome di dominio (FQDN) è formato dai nomi di tutte le label incontrate partendo dal nodo e salendo verso la root (up the tree), separati da punti
- Per la root non si usa alcuna label
- Un host si indica con il nome della foglia seguito dal punto e dal nome del dominio (es. `www.ibm.com.`)

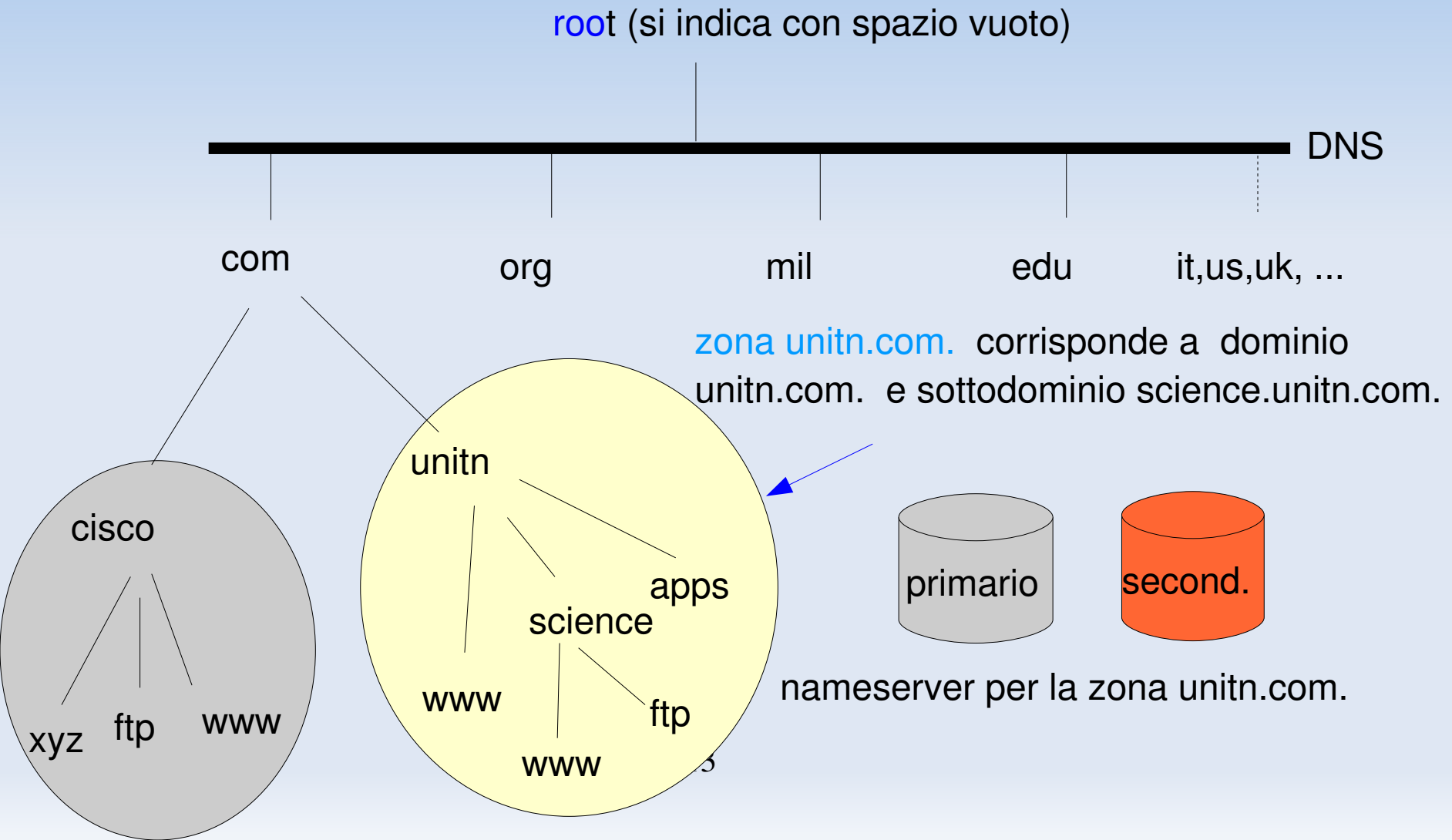
# DNS

## DNS (Domain Name System)

- Un nome di dominio viene assegnato da apposite Registration Authorities (per l'Italia è il CNR di Pisa) ad un'organizzazione (provider od utente diretto) che si assume in tal modo la relativa responsabilità di gestione
- L'organizzazione assegnataria di un nome di dominio dovrà esporre su Internet almeno un nameserver in grado di risolvere gli indirizzi di tutti gli host presenti in quel dominio (zona)
- Per ragioni di affidabilità si usano almeno due nameserver (primario e secondario) dei quali il secondo è la replica del primo
- Un assegnatario di un nome di dominio (es. unitn.it.) è autorizzato a usare anche nomi di sottodominio (es. fisica.unitn.it. ) in quanto non esiste possibilità di conflitto

# DNS

## DNS (Domain Name System)



# DNS

## DNS (Domain Name System)

- Si dice, in gergo tecnico, che un **nameserver** è **autoritativo per una certa zona**, ad indicare che è responsabile dei nomi di tutti gli host appartenenti ad un certo dominio ed a tutti i suoi sottodomini
- Il nameserver gestisce delle specifiche informazioni (RR resource record) delle quali le più importanti sono
  - **SOA** (Start of Authority): ne esiste uno per zona e riporta dei parametri di gestione
  - **NS** (name server): indica il nome dei nameserver (primario e secondari) dove reperire le informazioni di una zona (un record per host)
  - **A** (address): indica l'indirizzo IP (un record per host)

# DNS

## Esempio di zona definita in un nameserver

```
; zone fragment for example.com
; name servers in the same zone
$TTL 2d ; default TTL is 2 days
$ORIGIN example.com.
@      IN   SOA  ns1.example.com. hostmaster.example.com. (
        2003080800 ; serial number
        2h       ; refresh = 2 hours
        15M      ; update retry = 15 minutes
        3W12h   ; expiry = 3 weeks + 12 hours
        2h20M   ; minimum = 2 hours + 20 minutes
    )
; main domain name servers
    IN   NS   ns1.example.com.
    IN   NS   ns2.example.com.
; main domain mail servers
    IN   MX   mail.example.com.
; A records for name servers above
ns1     IN   A   192.168.0.3
ns2     IN   A   192.168.0.4
; A record for mail server above
mail    IN   A   192.168.0.5
....
```

# DNS

## DNS nameserver come processo

- Esistono anche dei records RR chiamati PTR per la gestione del mapping inverso (da indirizzo IP a nome)
- Il nameserver non è solo un database ossia non si limita a gestire i record RR necessari al mapping ma fornisce informazioni, secondo uno specifico protocollo, agli altri nameserver che le richiedono
- In effetti i nameserver forniscono un sistema di ricerca distribuito di informazioni

# DNS

## DNS processo ricorsivo di risoluzione dei nomi

Quando un client deve risolvere un nome:

- 1) interroga il suo nameserver
- 2) se il nameserver non possiede l'informazione (dominio richiesto diverso) viene innescata, in modo automatico, una ricerca a partire da uno dei root nameserver
- 3) Il root nameserver restituisce l'indirizzo IP di uno dei name server che gestiscono il dominio di primo livello contenuto nel dominio cercato (es. dns.nic.it. per [www.corriere.it](http://www.corriere.it))
- 4) Uno di questi nameserver fornisce l'indirizzo di uno dei nameserver che gestiscono il dominio di secondo livello (es. ns.ita.tip.net.)
- 5) Infine il nameserver così ottenuto è in grado di risolvere il nome

# DNS

## DNS processo ricorsivo di risoluzione dei nomi

- Nota:
  - I nameserver di root ossia quelli che contengono gli indirizzi dei nameserver dei domini di primo livello sono gestiti da organizzazioni specifiche distribuite nel mondo
  - I nameserver per i domini primo livello (es it.) sono di solito affidati ad un'organizzazione nazionale (es. CNR Pisa per Italia)
  - I nameserver per i domini di secondo livello e successivi sono in genere gestiti da provider o da organizzazioni pubbliche/private)

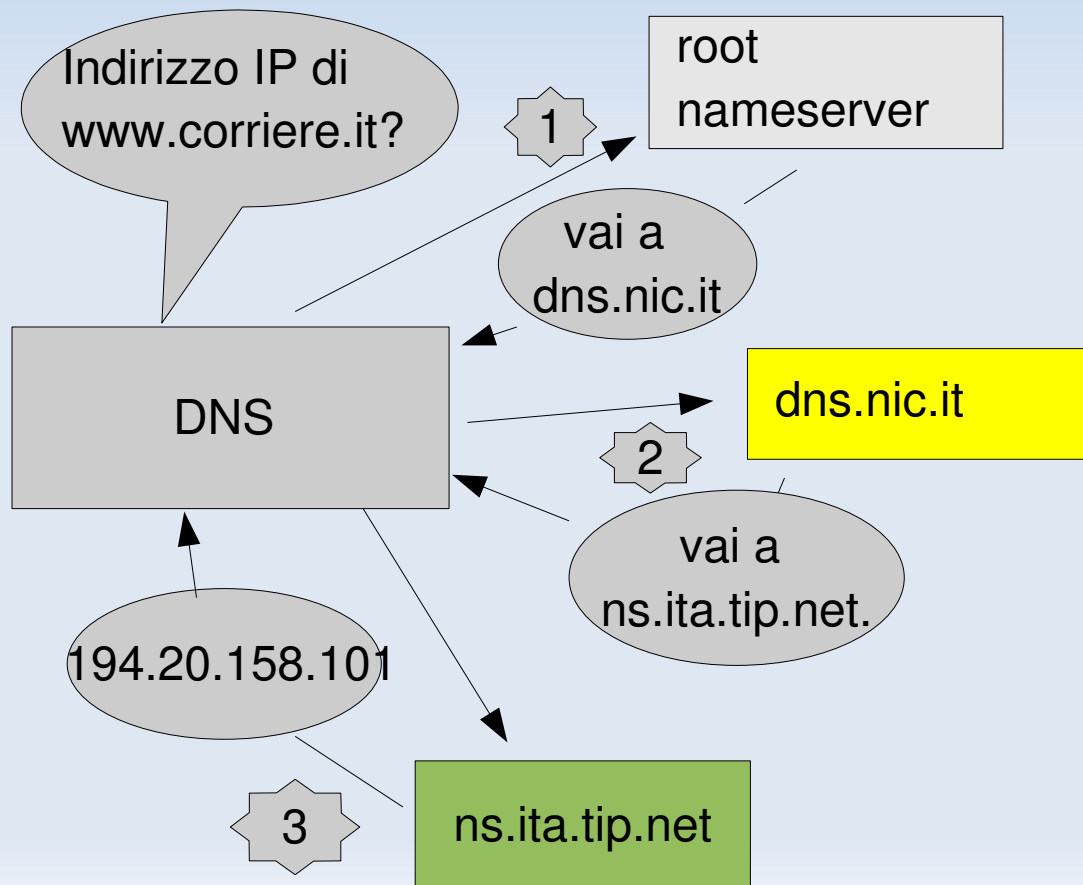
# DNS

## DNS processo ricorsivo di risoluzione dei nomi

- Nota:
  - Per ragioni prestazionali i nameserver mantengono in cache le informazioni trovate in modo da evitare di dover ricorrere a ricerche ricorsive per ogni richiesta

# DNS

Laboratorio : verifica del funzionamento del meccanismo di delega con comando dig



# DNS

## Laboratorio

- Verifica del processo ricorsivo di risoluzione di un nome
- Si userà il comando dig:

```
dig @<NomeNameServer> <nome cercato> +norec
```

Esempio

```
dig @dns.nic.it www.corriere.it +norec
```

# DNS

## Laboratorio

- Analisi di una ricerca mediante ethereal

Esempio

dig @dns.nic.it [www.corriere.it](http://www.corriere.it) +norec

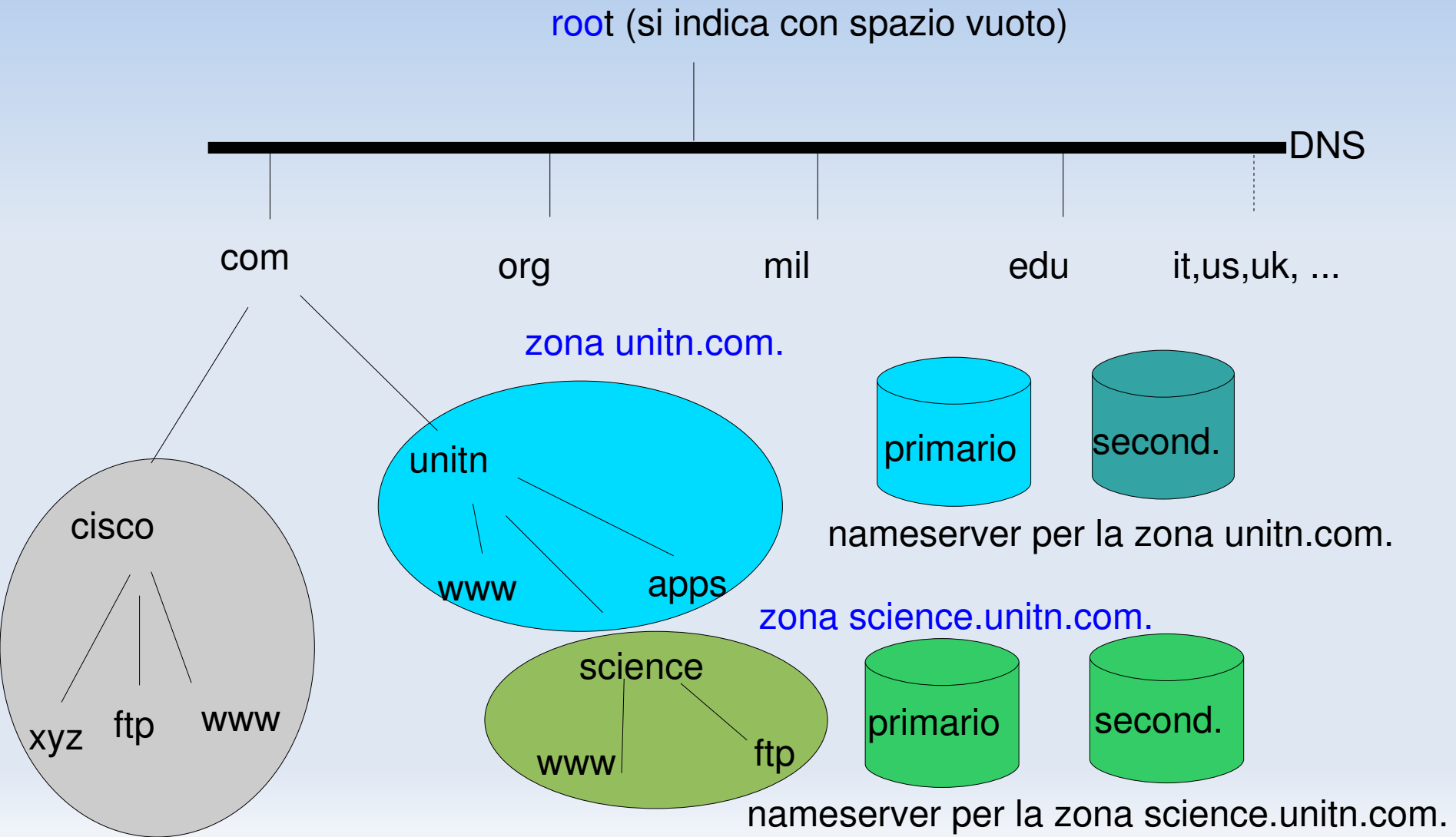
# DNS

## DNS (Domain Name System)

- Un'organizzazione può **delegare** ad un'altra un suo sottodominio.
- L'organizzazione delegata dovrà quindi gestire con un proprio nameserver la zona assegnata, che sarà formata dal sottodominio delegato e gli eventuali ulteriori sottodomini
- Ad esempio il dominio science.unitn.com. potrebbe essere delegato al dipartimento di scienze

# DNS

## DNS Zona delegata



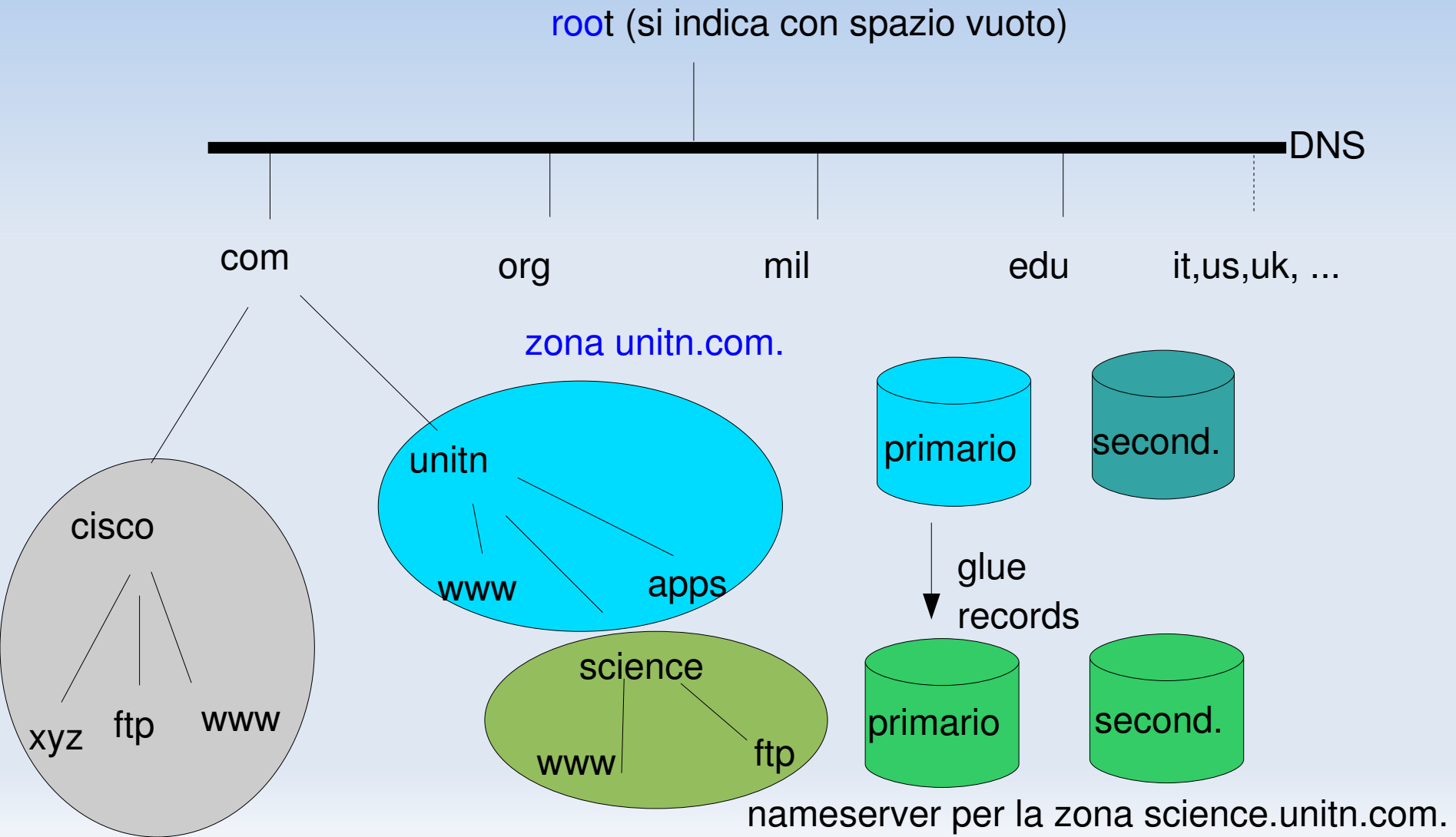
# DNS

## DNS (Domain Name System)

- Nel caso di zona delegata, sul nameserver del delegante dovranno essere presenti delle informazioni (glue records) che consentano di puntare, per la zona delegata, ai nameserver di competenza
- In effetti tutto il DNS si basa sul concetto di delega:
  - il nameserver del dominio di root delega ai nameserver dei domini di primo livello la relativa gestione dei nomi
  - ad esempio uno dei 13 root nameservers fornisce gli indirizzi dei nameservers delegati per la gestione degli indirizzi di primo livello (Top Level Domain)

# DNS

## DNS Zona delegata



# DNS

## DNS Vantaggi

- Distribuzione del carico di lavoro
- Ridondanza e quindi affidabilità
- Ogni organizzazione è direttamente responsabile dei suoi dati
- Impossibilità di nomi duplicati

# DNS

## DNS Va

- In sintesi ogni nameserver:
  - 1) Mantiene informazioni (RR Resource Records) degli host appartenenti alla sua zona
  - 2) può delegare ad altri nameserver la gestione di un suo sottodominio (zona)
  - 3) è in grado di interagire con gli altri DNS attraverso specifici protocolli in modo da recuperare, in modo iterativo, il mapping degli host appartenenti a zone per le quali esso NON è autoritativo
- Nota: per consentire alta affidabilità, il contenuto del nameserver viene replicato ad intervalli regolari in nameserver secondari

# DNS

## SINTESI

- ◆ La zona è costituita da un dominio e i suoi sottodomini che non sono a loro volta delegati, ed è quindi gestita da un unico nameserver
- ◆ L'organizzazione delegata dovrà allestire i propri nameserver così da garantire il mapping di tutti i nodi della zona sui quali è autoritativa (record di tipo A address per ogni host). Vedi esempio
- ◆ L'organizzazione delegante dovrà invece indicare, nei propri nameserver, i nomi dei server autoritativi per le zone delegate (record di tipo NS ed A di riferimento ai nameserver autoritativi per la zona) . Vedi esempio

# DNS

## SINTESI

- ◆ La zona è costituita da un dominio e i suoi sottodomini che non sono a loro volta delegati, ed è quindi gestita da un unico nameserver
- ◆ L'organizzazione delegata dovrà allestire i propri nameserver così da garantire il mapping di tutti i nodi della zona sui quali è autoritativa (record di tipo A address per ogni host). Vedi esempio
- ◆ L'organizzazione delegante dovrà invece indicare, nei propri nameserver, i nomi dei server autoritativi per le zone delegate (record di tipo NS ed A di riferimento ai nameserver autoritativi per la zona) . Vedi esempio

# DNS

## SINTESI

**// named.conf file fragment**

.....

**zone "example.com" in{**

**type master;**

**file "master/master.example.com";**

**// explicitly allow slave**

**allow-transfer {192.168.0.4};**

**};**

**// optional - we act as the slave (secondary) for the delegated domain**

**zone "us.example.com" IN {**

**type slave;**

**file "slave/slave.us.example.com";**

**masters {10.10.0.24};**

**};**

# DNS

## SINTESI

```
; zone fragment for example.com
; name servers in the same zone
$TTL 2d ; default TTL is 2 days
$ORIGIN example.com.
@      IN   SOA  ns1.example.com. hostmaster.example.com. (
    2003080800 ; serial number
    2h        ; refresh = 2 hours
    15M       ; update retry = 15 minutes
    3W12h     ; expiry = 3 weeks + 12 hours
    2h20M     ; minimum = 2 hours + 20 minutes
    )
; main domain name servers
    IN   NS   ns1.example.com.
    IN   NS   ns2.example.com.
; main domain mail servers
    IN   MX   mail.example.com.
; A records for name servers above
ns1     IN   A   192.168.0.3
ns2     IN   A   192.168.0.4
; A record for mail server above
mail    IN   A   192.168.0.5
....
```

# DNS

## SINTESI

**; sub-domain definitions**

**\$ORIGIN us.example.com.**

**; we define two name servers for the sub-domain**

**@ IN NS ns3.us.example.com.**

**; the next name server points to ns1 above**

**IN NS ns1.example.com.**

**; sub-domain address records for name server only - glue record**

**ns3 IN A 10.10.0.24 ; 'glue' record**

# DNS

## SINTESI

*// named.conf file fragment for nameserver authoritative for us.example.com*

```
zone "us.example.com" in{  
type master;  
file "master/master.us.example.com";  
    // explicitly allow slave  
allow-transfer {192.168.0.3};  
};
```

# DNS

## SINTESI

// named.conf file fragment

; zone fragment for sub-domain us.example.com

; name servers in the same zone

\$TTL 2d ; default TTL = 2 days

\$ORIGIN us.example.com.

@ IN SOA ns3.us.example.com. hostmaster.us.example.com. (

2003080800 ; serial number

2h ; refresh = 2 hours

15M ; update retry = 15 minutes

3W12h ; expiry = 3 weeks + 12 hours

2h20M ; minimum = 2 hours + 20 minutes

)

; sub-domain name servers

IN NS ns3.us.example.com.

IN NS ns1.example.com.

; sub-domain mail server

IN MX 10 mail.us.example.com.

; A records for name servers above

ns3 IN A 10.10.0.24

ns1.example.com. IN A 192.168.0.3 ; 'glue' record

; A record for mail server above

mail IN A 10.10.0.25

ftp IN A 10.10.0.28

glue record non  
strettamente  
necessario

# DNS

## Esempio di zona unitn.org.

```
•; BIND data file for unitn.org
•;
•$TTL      777777
•@ IN SOA server.unitn.org. root.claudiocovelli.org. (
•          1; Serial
•          604800; Refresh
•          86400; Retry
•          2419200; Expire
•          777777 ) ; Negative Cache TTL
•;
•@ IN NS server 36
•@ IN MX 10 mail
```

nome del server autoritativo per la zone unitn.org.

indirizzo di email del responsabile della zona

parametri di funzionamento della zona

name server autoritativo e mail server della zona

records :  
es. [www.unitn.org](http://www.unitn.org). => 194.209.20.4

# DNS

## I 13 Root Servers

- |                         |                |
|-------------------------|----------------|
| 1) A.ROOT-SERVERS.NET.  | 198.41.0.4     |
| 2) B.ROOT-SERVERS.NET.  | 192.228.79.201 |
| 3) C.ROOT-SERVERS.NET.  | 192.33.4.12    |
| 4) D.ROOT-SERVERS.NET.  | 128.8.10.90    |
| 5) E.ROOT-SERVERS.NET.  | 192.203.230.10 |
| 6) F.ROOT-SERVERS.NET.  | 192.5.5.241    |
| 7) G.ROOT-SERVERS.NET.  | 192.112.36.4   |
| 8) H.ROOT-SERVERS.NET.  | 128.63.2.53    |
| 9) I.ROOT-SERVERS.NET.  | 192.36.148.17  |
| 10) J.ROOT-SERVERS.NET. | 192.58.128.30  |
| 11) K.ROOT-SERVERS.NET. | 193.0.14.129   |
| 12) L.ROOT-SERVERS.NET. | 198.32.64.12   |
| 13) M.ROOT-SERVERS.NET. | 202.12.27.33   |

# DNS

## laboratorio: allestimento di un name server per la propria LAN

- Installare il programma bind
- aggiornare il file /etc/hosts con gli indirizzi IP che vanno risolti prima di ogni accesso al nameserver
- aggiornare il file /etc/resolv.conf facendolo puntare all'indirizzo IP del nameserver

# DNS

## laboratorio: allestimento di un name server per la propria LAN

- inserire la zona per le quali tale nameserver sarà autoritativo nel file di testo `/etc/bind/named.conf.local`
- definire la zona in `/etc/bind` usando il nome di file richiamato in `named.conf.local`
- lanciare bind usando il comando `/etc/init.d/bind restart`
- effettuare il test con il comando `dig`

# DNS

## TLD (Top Level Domains)

- com (commercial)
- edu (educationa)
- gov (government; es. nasa.gov)
- mil (military)
- net (network infrastructure)
- org (not commercial organizatios)
- int (international)
- arpa (usato per reverse mapping)
- country code (it,us,uk, de etc). ISO 3166
- new (es. aero, biz, coop, info, museum, eu etc)