

Università di Roma Tor Vergata  
Corso di Laurea triennale in Informatica  
**Sistemi operativi e reti**  
A.A. 2016-17

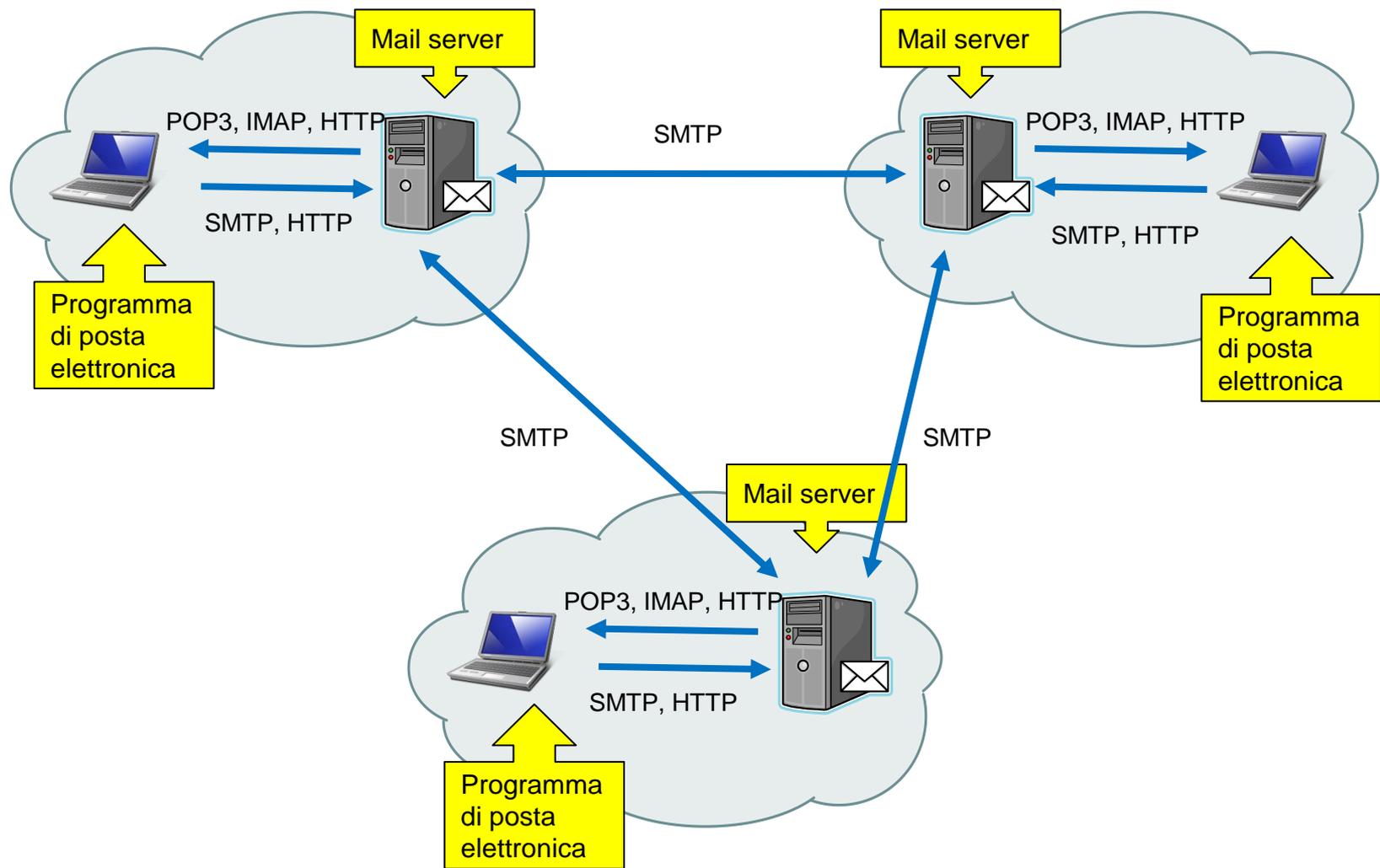
Pietro Frasca

Parte II: Reti di calcolatori  
Lezione 8 (32)

Venerdì 31-03-2017

# Protocolli di accesso alla posta

- L'SMTP è principalmente usato per trasferire i messaggi dal server del mittente al server del destinatario.
- L'SMTP è anche usato per trasferire messaggi da un programma di posta del mittente alla suo account sul server di posta elettronica.
- L'SMTP non consente di trasferire messaggi dalla mailbox dell'utente al suo programma di posta.
- Attualmente esistono vari protocolli di accesso alla posta, tra i quali:
  - **POP3** (*Post Office Protocol, protocollo dell'ufficio postale, versione 3*),
  - **IMAP** (*Internet Mail Access Protocol, protocollo di accesso alla posta Internet*) e
  - **HTTP**.
- La figura seguente mostra i protocolli usati per la posta in Internet.



# POP3

- Il POP3, definito nella RFC 1939, è un protocollo di accesso per la posta elettronica molto utilizzato. Ha un'architettura client/server e utilizza il TCP e la **porta 110**.
- Dopo aver instaurato la connessione TCP, il POP3 esegue tre fasi: **autorizzazione**, **transazione** e **aggiornamento**.
- Durante la prima fase di **autorizzazione**, il client invia lo username e la password per ottenere l'accesso alla sua mailbox e quindi scaricare i messaggi di posta. La fase di autorizzazione ha due comandi principali:
  - **user *username***
  - **pass *password***
- Durante la seconda fase, **transazione**, il client può inviare comandi per scaricare i messaggi. Durante questa fase il client può anche selezionare i messaggi da eliminare.

- Nella fase di transazione, il client invia comandi e il server risponde a ciascun comando. Ci sono due possibili risposte:
  - **+OK** (qualche volta seguita da dati dal server al client), usata dal server per indicare che i comandi precedenti sono corretti;
  - **-ERR**, usata dal server per indicare che nei precedenti comandi c'è qualche errore.
- I comandi principali di questa fase sono:
  - **list**, per ottenere l'elenco dei messaggi presenti nella mailbox;
  - **retr n**, per scaricare il messaggio con indice n;
  - **dele n**, per cancellare il messaggio di indice n.
- Un'applicazione di posta che usa POP3 generalmente può essere configurata per funzionare nella modalità "**scarica ed elimina**" (**download-and-delete**) o per "**scarica e mantieni**" (**download-and-keep**). La sequenza dei comandi inviati dal client POP3 dipende da quale di queste due modalità viene usata.

- Nel modo download-and-delete, il client invia i comandi **list**, **retr**, e **dele**.
- La terza fase, **aggiornamento**, avviene dopo che il client ha inviato il comando **quit**, per chiudere la sessione POP3. Prima di chiudere la sessione, il server aggiorna lo stato della casella di posta eliminando eventuali messaggi che erano stati marcati per la cancellazione.
- Con telnet è possibile instaurare una sessione con un server POP3, come descritto di seguito.

```
> telnet reti.uniroma2.it 110
Trying reti.uniroma2.it...
Connected to reti.uniroma2.it.
Escape character is '^]'.
+OK QPOP Modified by Compaq (version 3.0.2) at
  reti.uniroma2.it starting.
  <407574.1206554653@reti.uniroma2.it>
user frasca
+OK Password required for frasca.
pass miapassword
+OK frasca has 299 visible messages (0 hidden) in
  53421318 octets.
list
+OK 299 visible messages (53421318 octets)
1 550
2 10670
3 2723
4 8329
... ..
```

**retr 1**

+OK 550 octets

Date: 27 Mar 2008 16:05:11 +0100

From: white@hi.unibr.uk

Subject: test pop3

Message-ID: <1206630311@reti.uniroma2.it>

...

X-UIDL: :\_@!!H[K"!HP&!!40T!!

...

Bla bla bla bla bla bla bla

Bla bla bla .....

**dele 292**

+OK Message 292 has been deleted.

**quit**

+OK Pop server at reti.uniroma2.it signing off.

Connection closed by foreign host.

- il server POP3 esegue la fase di aggiornamento e rimuove il messaggio 292 dalla casella di posta dopo aver ricevuto il comando **quit**.
- E' possibile annullare la cancellazione di un messaggio (prima di inviare il comando quit) con il comando **RSET**.
- Il POP3 possiede anche alcuni comandi opzionali tra i quali, molto utile, il comando **TOP**, che consente di scaricare solo le **prime N righe** del corpo di un messaggio, oltre all'intestazione. Ad esempio, **TOP 10 5** trasferisce dal server le prime 5 righe del messaggio numero **10**. Indicando **0** nel parametro delle righe POP3 scarica solo l'intestazione.
- Durante una sessione POP3, il server mantiene alcune informazioni di stato come ad esempio gli indici dei messaggi selezionati per l'eliminazione.
- Il POP3 non permette di creare cartelle remote e di ordinare i messaggi in cartelle.
- Tuttavia, le applicazioni di posta che usano il POP3 sono realizzate in modo da organizzare i messaggi scaricati in cartelle nel file system locale dell'utente. Questo funzionamento può essere un problema per gli utenti che leggono la posta da più host, poiché è preferibile avere un unico ordinamento delle cartelle direttamente sul server remoto.

# IMAP

- Un altro protocollo di accesso alla posta è **IMAP** (**Internet Mail Access Protocol**, *Protocollo di Accesso alla Posta Internet*), è definito nella RFC 2060. IMAP utilizza il TCP e la porta 143.
- IMAP ha molte più potenzialità rispetto a POP3, ma è anche molto più complesso.
- Il server IMAP consente di salvare i messaggi in cartelle remote. Un messaggio, quando arriva al server IMAP, viene memorizzato nella cartella **INBOX** dell'utente destinatario. Successivamente, l'utente può leggere i messaggi ricevuti, creare nuove cartelle e organizzare i messaggi in modo personalizzato, cancellarli e così via.

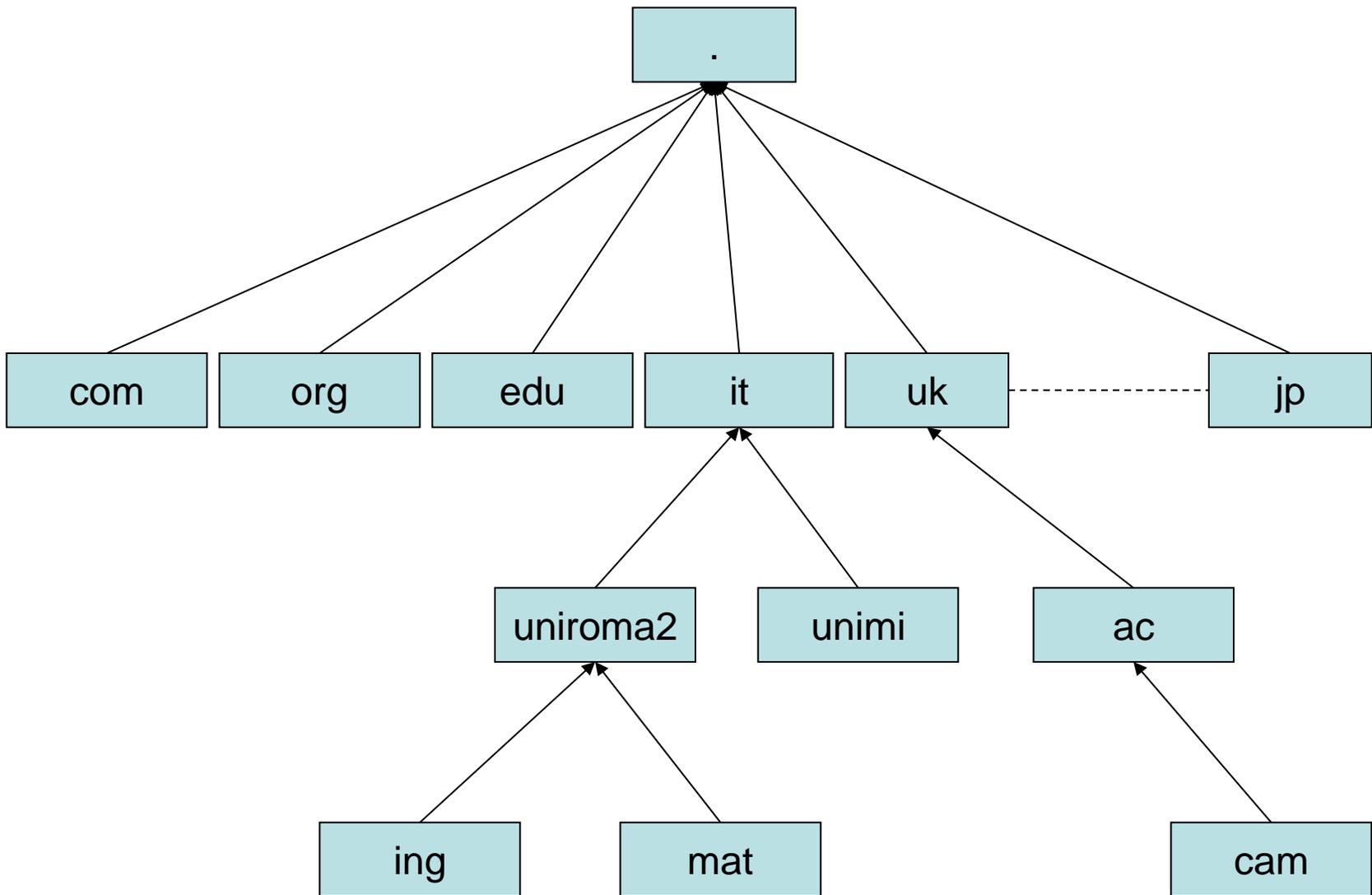
- IMAP ha anche comandi per ricercare nelle cartelle remote messaggi che soddisfano determinati criteri.
- Un server IMAP conserva informazioni di sessione, come ad esempio, i nomi delle cartelle create e la corrispondenza tra messaggi e cartelle.
- Un'altra caratteristica di IMAP è che possiede comandi che consentono di ottenere solo alcune parti dei messaggi. Per esempio, un client può estrarre solo l'intestazione di un messaggio, o solo una parte di un messaggio MIME multi parte. Questa caratteristica è utile quando la connessione tra client e server di posta è a bassa velocità, come ad esempio in una connessione dial-up a 56 Kbit/sec.

# Posta elettronica con HTTP

- E' possibile accedere alla posta elettronica anche attraverso i browser Web. In questo caso un'applicazione web gestisce le caselle postali degli utenti sul server e i messaggi sono trasferiti dall'HTTP in entrambe le direzioni, da browser verso server e da server verso il browser.
- Molte applicazioni web per la gestione di posta elettronica usano un server IMAP per fornire le funzionalità delle cartelle remote.

# DNS (*Domain Name System*)

- In Internet, gli host sono identificati dall'indirizzo IP e spesso anche da nomi in quanto sono più facili da ricordare.
- Ad esempio, nell'IPv4, un indirizzo è lungo 32 bit e si scrive nella forma detta **decimale puntata**, costituita da 4 cifre decimali, con valori compresi tra 0 e 255, separate da un punto. Un esempio di indirizzo IPV4 è 160.80.13.56.
- Un indirizzo IP ha una struttura gerarchica. La prima parte dell'indirizzo specifica la rete, mentre la seconda specifica il particolare host. Ad esempio 160.80. identifica la rete mentre 13.56 specifica l'host all'interno della rete.
- Ad una rete viene associato un nome (**dominio**). Ad esempio **uniroma2.it** è il dominio della rete **160.80**.
- Anche i nomi di dominio hanno una struttura gerarchica, come mostrato nella figura seguente.



Struttura gerarchica dei nomi di dominio

# Servizi forniti dal DNS

- Il **DNS** (***Domain Name System***) è un protocollo che fornisce vari servizi, il principale dei quali converte i nomi degli host (**hostname**) in **indirizzi IP**. Questa operazione è detta **risoluzione degli indirizzi**.
- Il DNS utilizza **UDP** e la **porta 53**. Tuttavia se la risposta del server DNS supera i 512 byte, questo risponde con un particolare messaggio che indica al client di ripetere la richiesta utilizzando il TCP. Anche con il TCP la porta usata è la 53.
- Il DNS è usato da qualsiasi programma di rete, e anche dagli altri protocolli dello strato di applicazione, come HTTP, SMTP, telnet e FTP.
- Per i name server si usano spesso sistemi operativi Unix dotati del software **named** che è contenuto nel pacchetto **BIND** (**Berkeley Internet Name Domain**).
- Il DNS oltre alla risoluzione degli indirizzi, fornisce alcuni altri importanti servizi:

- **Alias degli hostname.** Un host oltre al nome può avere uno o più alias. Per esempio, l'hostname [www.informatica.uniroma2.it](http://www.informatica.uniroma2.it) ha l'alias [www.cs.uniroma2.it](http://www.cs.uniroma2.it). In questo caso, l'hostname [www.informatica.uniroma2.it](http://www.informatica.uniroma2.it) è chiamato **hostname canonico**.  
Generalmente gli alias degli hostname, se usati, sono più semplici da ricordare dell'hostname canonico.  
Un'applicazione che usa il DNS può ottenere l'hostname canonico fornendo l'alias o l'indirizzo IP dell'host.
- **Alias dei server di posta.** Il DNS permette che il server di posta e il Web server (o altri servizi) di un'organizzazione abbiano lo stesso hostname.
- **Distribuzione del carico.** Il DNS svolge anche il compito di distribuire il carico dei dati copiati su più server web. I siti web molto visitati sono spesso replicati su vari server detti **mirror (specchio)**, ciascuno dei quali ha un diverso indirizzo IP. In tal caso, per ogni hostname canonico, il DNS memorizza un **gruppo di indirizzi IP**, costituito dagli indirizzi IP di ciascuno dei server mirror. Quando i client inviano una richiesta al DNS per avere un indirizzo di un server web mirror, il server DNS risponde inviando l'intero insieme di indirizzi IP, ma ad ogni nuova richiesta ruota l'ordine degli indirizzi.

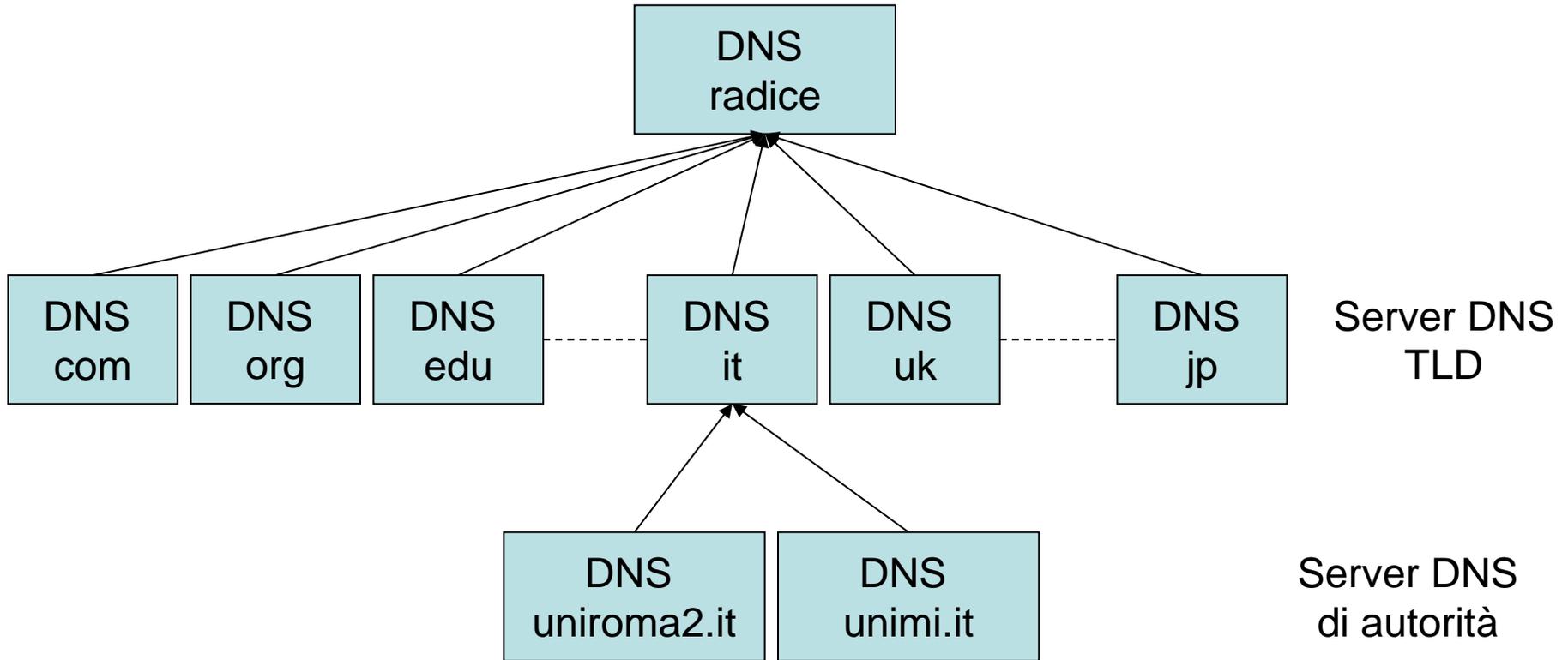
Poiché, generalmente, un client invia il suo messaggio di richiesta HTTP all'indirizzo IP del primo indirizzo del gruppo, la rotazione degli indirizzi permette di distribuire il traffico tra i vari mirror.

## Funzionamento del DNS

- Per ottenere la risoluzione dell'indirizzo, un'applicazione eseguirà il lato client del DNS, specificando l'hostname che deve essere tradotto. Ad esempio in ambiente c/Unix la System Call per la traduzione è **gethostbyname (hostname )**.
- Il client DNS invia un messaggio di richiesta al server DNS e questo risponde al client con un messaggio di risposta che contiene il numero IP desiderato. Il numero IP viene successivamente passato all'applicazione che lo ha richiesto.

# Database distribuiti e gerarchici

- Dato l'altissimo numero di host connessi a Internet, nessun server DNS ha le corrispondenze di tutti gli host, che sono invece distribuite tra un grande numero di server DNS, organizzati in modo gerarchico e distribuiti in tutto il mondo.
- In prima approssimazione, possiamo classificare i server DNS in tre categorie:
  - **server DNS radice (ROOT),**
  - **server DNS top-level domain (TLD)**
  - **server DNS di competenza (di autorità amministrativa)**
- Le tre classi di server DNS sono organizzate gerarchicamente come mostrato nella figura seguente.



Gerarchia (parziale) di server DNS

- **Server radice (*root nameserver*)**. I root nameserver sono 13 in tutto il mondo (etichettati da A a M), di cui 10 negli USA, due in Europa (Inghilterra e Svezia) ed uno in Giappone. Per aumentare l'affidabilità ciascuno dei server DNS è in realtà un cluster di server replicati. Essi possiedono l'elenco dei server di tutti i domini di primo livello (TLD) riconosciuti.
- **Server DNS di primo livello (Top Level Domain, TLD)**. Questi server si occupano dei domini di alto livello quali **edu**, **net**, **com**, **org**, e **gov**, e di tutti i **domini nazionali** come **it**, **fr**, **uk**, **jp** etc..
- **Server di autorità (o di competenza) (*authoritative server*)**. Le organizzazioni che desiderano rendere accessibili pubblicamente i propri host, mediante il nome, devono registrare tali host in server DNS. La maggior parte delle grandi organizzazioni e delle università gestiscono i propri DNS di autorità. Altre organizzazioni si rivolgono a fornitori di servizi per registrare queste associazioni su un server DNS. Per la grande importanza che ha il DNS i server di autorità sono generalmente due, detti server primario e secondario (di backup).

- A. Verisign Los Angeles CA
- C. Cogent, Herndon, VA
- D. U Maryland College Park, MD
- G. US DoD Columbus, OH
- H. ARL Aberdeen, MD
- J. Versign, Dulles VA

- E. NASA Mt View, CA
- F. Internet Software C. Palo Alto, CA

- I. NetNod Stockholm
- K. Ripe London

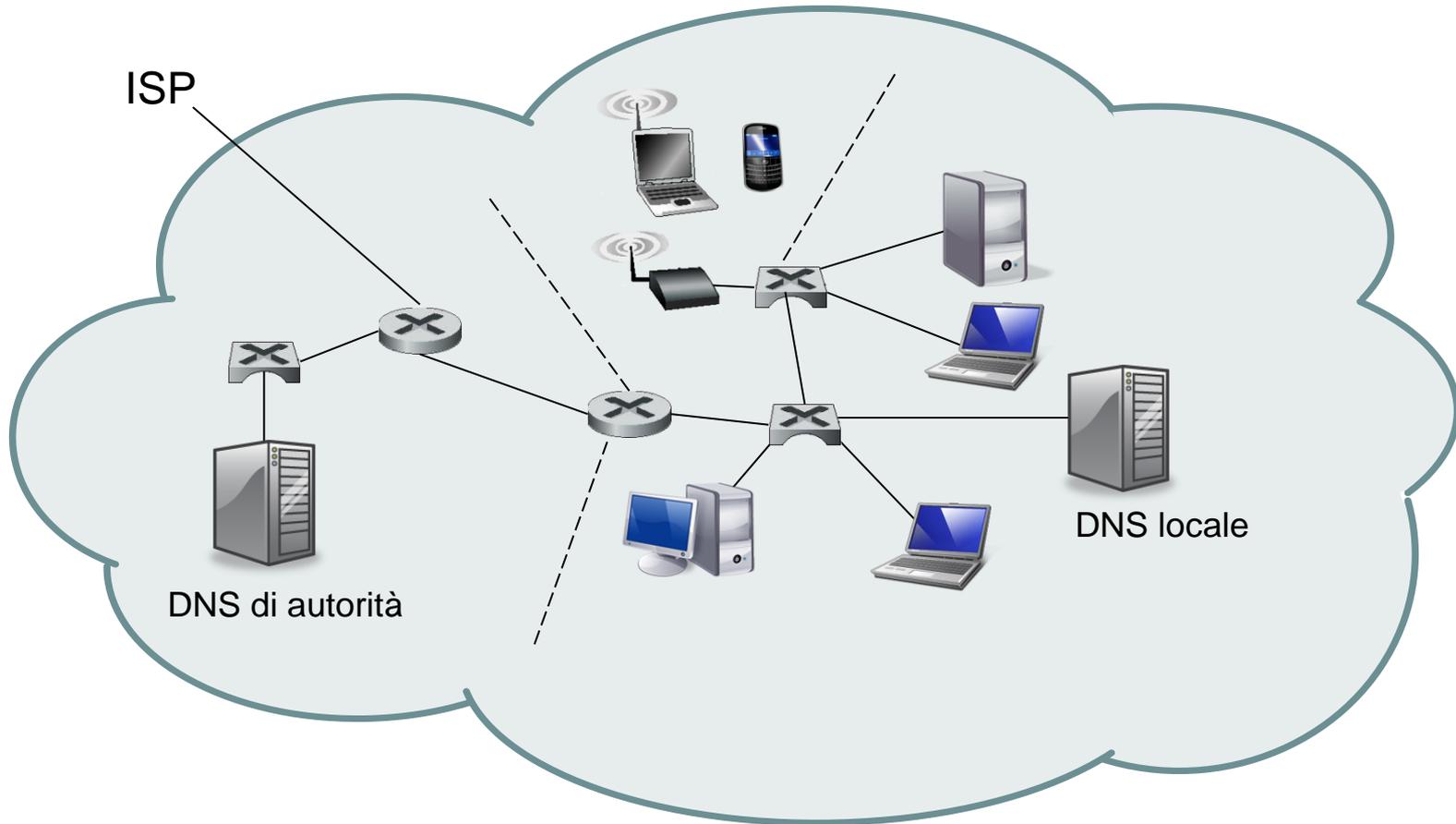
- B. USC-ISI Marina del Rey, CA
- L. ICANN Marina del Rey, CA

- M. WIDE Tokyo

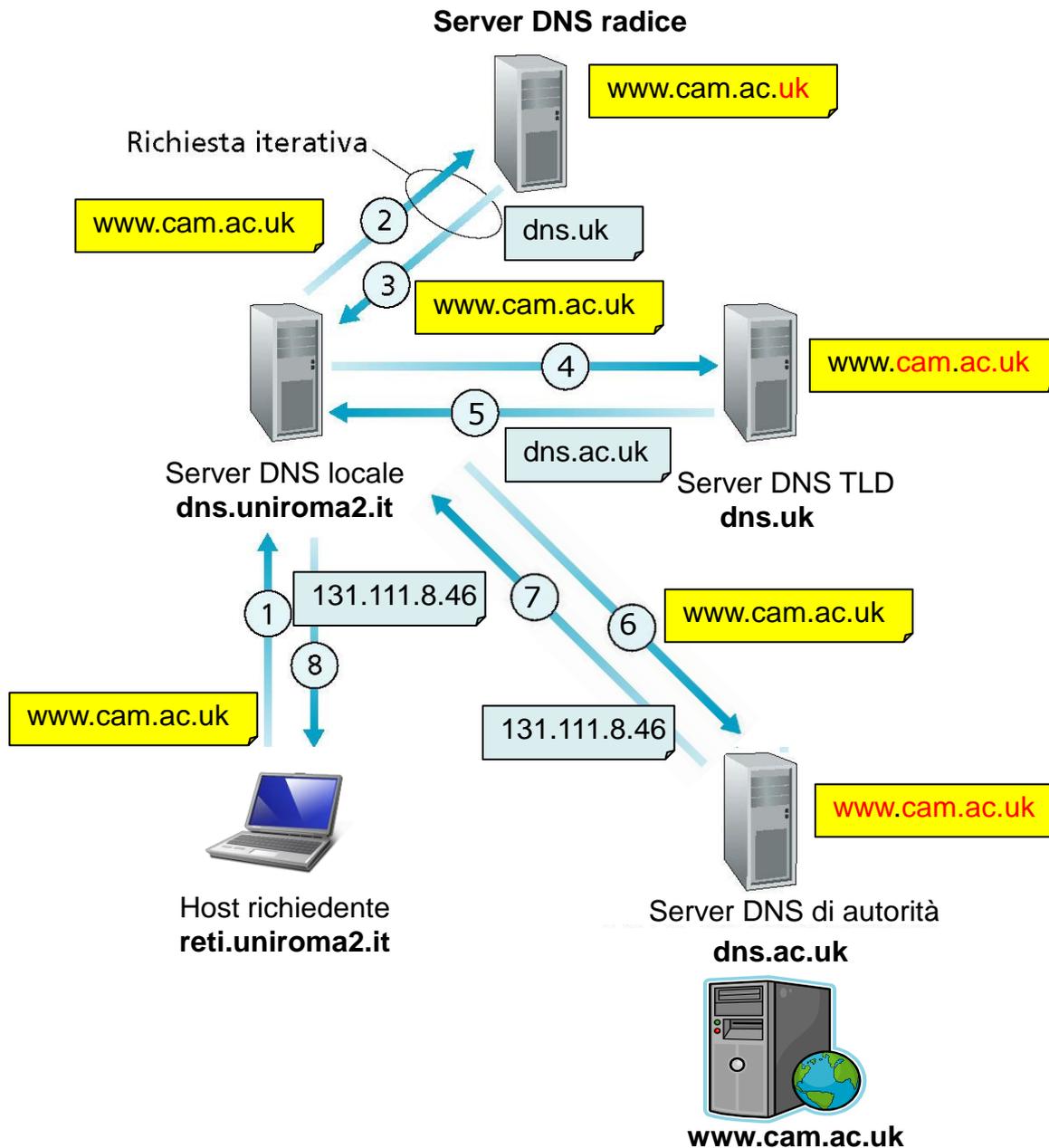


- Le grandi organizzazioni, che hanno reti estese, spesso utilizzano oltre al server di autorità, DNS locali (detti anche **default name server**). Per velocizzare la risoluzione degli indirizzi per un elevato numero di client, un server DNS locale è installato generalmente nella parte di rete cui sono connessi gli host.

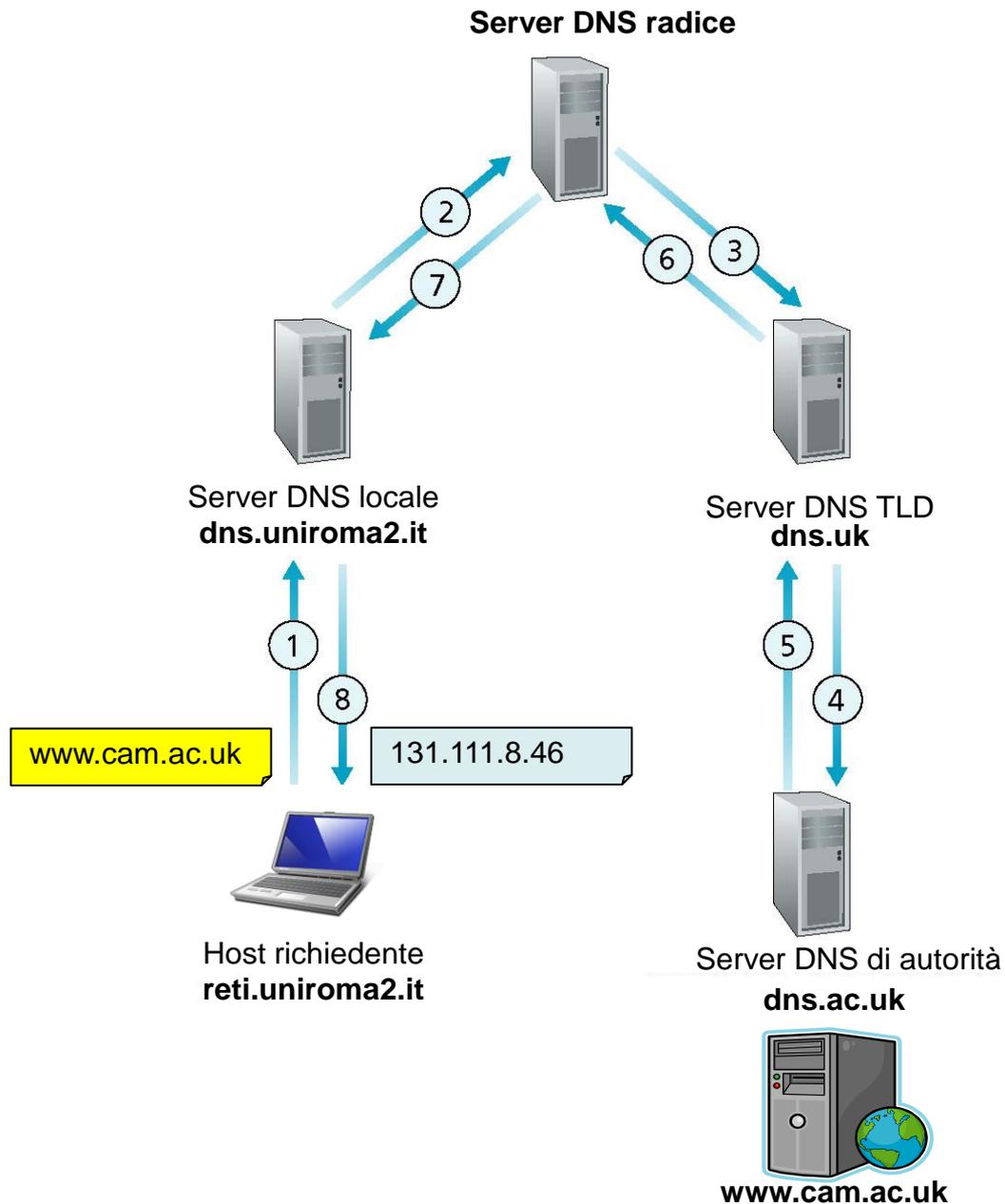
## Alcuni livelli di DNS



- Quando un host accede ad Internet tramite un ISP, un server dotato di **DHCP (Dynamic Host Configuration Program)** invia automaticamente all'host un insieme di parametri tra i quali l'indirizzo IP, mediante cui l'host è identificato in Internet e l'indirizzo di almeno un server **DNS locale** (generalmente due).
- Quando un host richiede una risoluzione di indirizzo, la richiesta DNS viene inviata al server DNS locale, il quale la rinvia in una gerarchia di server DNS.
- Facciamo un esempio. Supponiamo che l'host **reti.uniroma2.it** richieda l'indirizzo IP di un web server dell'università di Cambridge **www.cam.ac.uk**. Supponiamo, inoltre, che il server locale DNS del dominio uniroma2.it sia **dns.uniroma2.it**, mentre un server di autorità per **www.cam.ac.uk** sia **dns.ac.uk**. Come mostrato nella figura, l'host reti.uniroma2.it prima invia un messaggio di richiesta, contenente il nome da tradurre **www.cam.ac.uk**, al proprio server locale dns.uniroma2.it. Il server locale inoltra il messaggio di richiesta a un server radice il quale analizza, da destra verso sinistra, l'indirizzo da tradurre e in base al suffisso **uk** restituisce al server locale un elenco di indirizzi IP per i server TLD responsabili di uk.



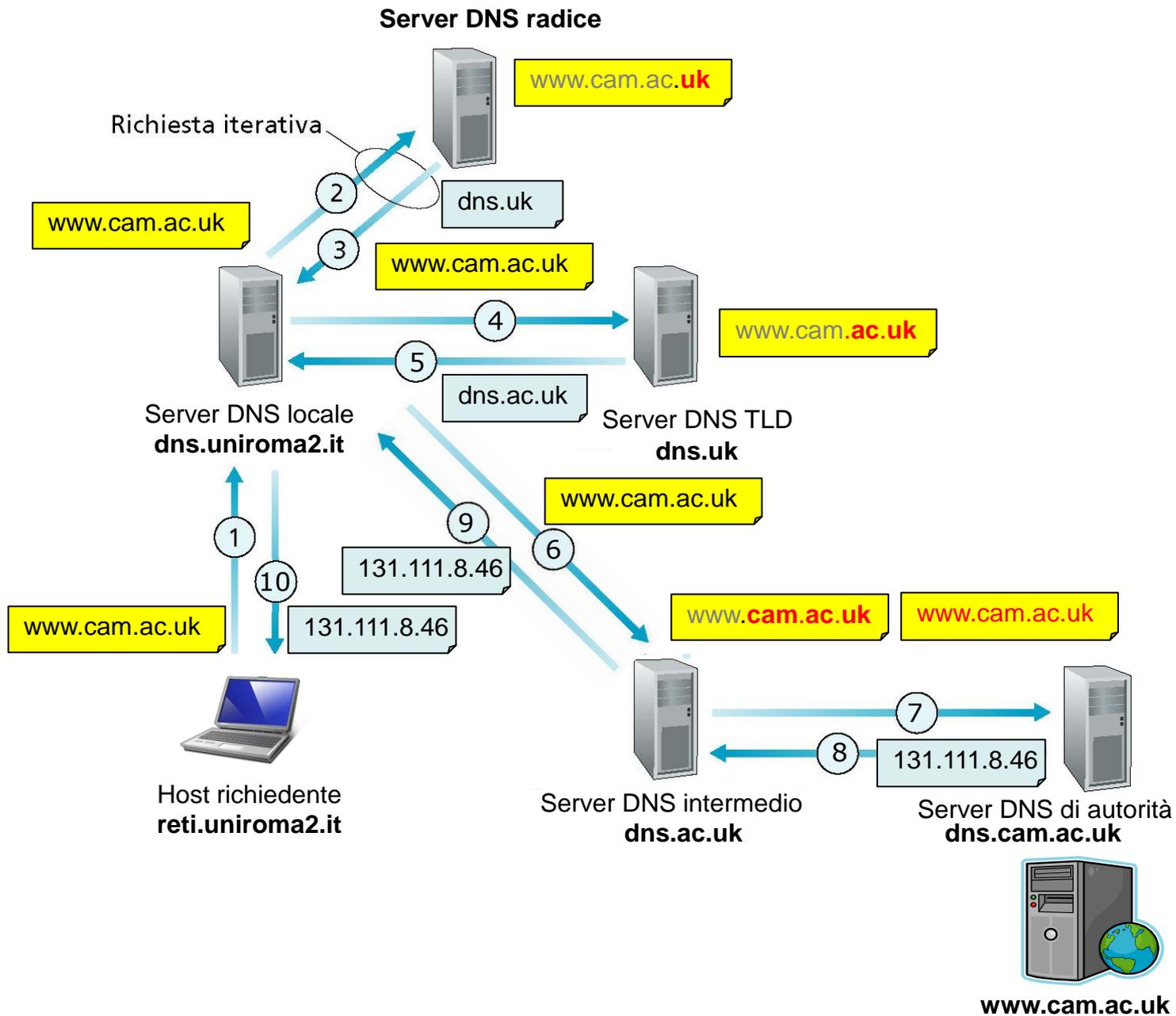
## Interazione tra DNS (funzionamento tipico)



## Richieste DNS ricorsive

- Il server locale rinvia quindi il messaggio di richiesta a uno di questi ultimi.
- Il server **TLD** considera ora il suffisso **ac.uk** e risponde con l'indirizzo IP del server di autorità per il server `www.cam.ac.uk`, ossia **dns.ac.uk**.
- Infine, il server DNS locale rimanda il messaggio di richiesta direttamente a `dns.ac.uk`, che risponde con l'indirizzo IP di `www.cam.ac.uk`.
- Si può notare che in questo esempio, per ottenere la risoluzione dell'indirizzo, sono stati inviati quattro messaggi di richiesta e quattro messaggi di risposta, per un totale di otto messaggi.
- Nel esempio abbiamo supposto che il server TLD conoscesse il server di autorità per quel dato nome, ma in generale non è così. E' possibile che il server TLD conosca solo un server DNS intermedio, il quale a sua volta conosce il server di autorità relativo all'hostname.
- Supponiamo ora che oltre al name server `dns.ac.uk` sia presente anche **dns.cam.ac.uk** il quale ora sia esso di **autorità per** `www.ca.ac.uk`

- Come mostrato nella figura seguente, quando il name server radice riceve un richiesta per un hostname che termina con uk, esso invia la richiesta al name server dns.uk. Questo name server invia tutte le richieste relative agli hostname che terminano con cam.ac.uk al name server dns.cam.ac.uk, che è il name server di autorità per gli hostname con il sottodominio cam.ac.uk. Il name server di autorità invia la risoluzione desiderata al server DNS intermedio, dns.ac.uk, che la passa al name server radice, che la passa al name server locale, dns.uniroma2.it, questo, a sua volta, invia la risoluzione all'host reti.uniroma2.it che ha fatto la richiesta. In questo esempio, si sono inviati dieci **messaggi DNS**.
- In realtà, per tradurre un singolo hostname possono essere inviati anche più di dieci messaggi DNS: ci possono essere due o più server DNS intermedi nel percorso tra il server radice e il server di competenza.



## Cache DNS

- Abbiamo visto che i server DNS si scambiano informazioni in modo gerarchico. Per ridurre il traffico di rete, generato dai messaggi di richiesta e di risposta DNS, e diminuire i tempi di risposta per le risoluzioni degli indirizzi, i DNS utilizzano una memoria cache nella quale memorizzano le informazioni che hanno precedentemente richiesto.
- Generalmente mantengono le coppie [hostname, indirizzo ip] per 2 giorni.

# Record DNS

- Per ottenere il funzionamento descritto precedentemente, i name server utilizzano tabelle la cui riga è detta **record di risorsa (RR, Resource Record)** che può essere di vario tipo. I campi più significativi di un record di risorsa sono i seguenti:

Tipo	Nome	Valore	TTL
------	------	--------	-----

- **TTL** è il tempo di vita del record di risorsa che definisce un intervallo di tempo scaduto il quale il record sarà rimosso dalla cache. Negli esempi seguenti non considereremo il campo TTL.
- I significati di **Nome** e **Valore** dipendono dal campo **Tipo**.

- Se **Tipo = A** (*Address*), allora:
  - il campo **Nome** contiene **il nome di un host**
  - **Valore** contiene il suo **indirizzo IP**.
  - Quindi, un record di **tipo A** fornisce la corrispondenza tra nome di un host e il suo indirizzo IP.
  - Per esempio  
**(A, reti.uniroma2.it, 160.80.30.130)** è un record di tipo A.
- Se **Tipo = NS** (*Name Server*), allora:
  - **Nome** è il nome di un dominio (come ad esempio **uniroma2.it**)
  - **Valore** è il nome di un **DNS di autorità** per quel dominio.
  - Questo record è usato per instradare le richieste DNS ad altri DNS.
  - Per esempio:  
**(NS, uniroma2.it, dns.uniroma2.it)** è un record di tipo **NS**.

- Se **Tipo = CNAME** (*Canonical Name*), allora:
  - **Nome** è un **alias**
  - **Valore** è il **nome canonico di un host**.
  - Questo record può fornire all'host richiedente il nome canonico di un hostname.
  - Per esempio:

**(CNAME, www.cs.uniroma2.it,  
www.informatica.uniroma2.it)**

- Se **Tipo=MX** (*Mail eXchanger*) , allora:
  - **Valore** è il nome canonico di un server di posta elettronica e
  - il campo **Nome** contiene il suo **alias**.
  - Un esempio di record MX è il seguente:

**(MX, uniroma2.it, mail.uniroma2.it).**

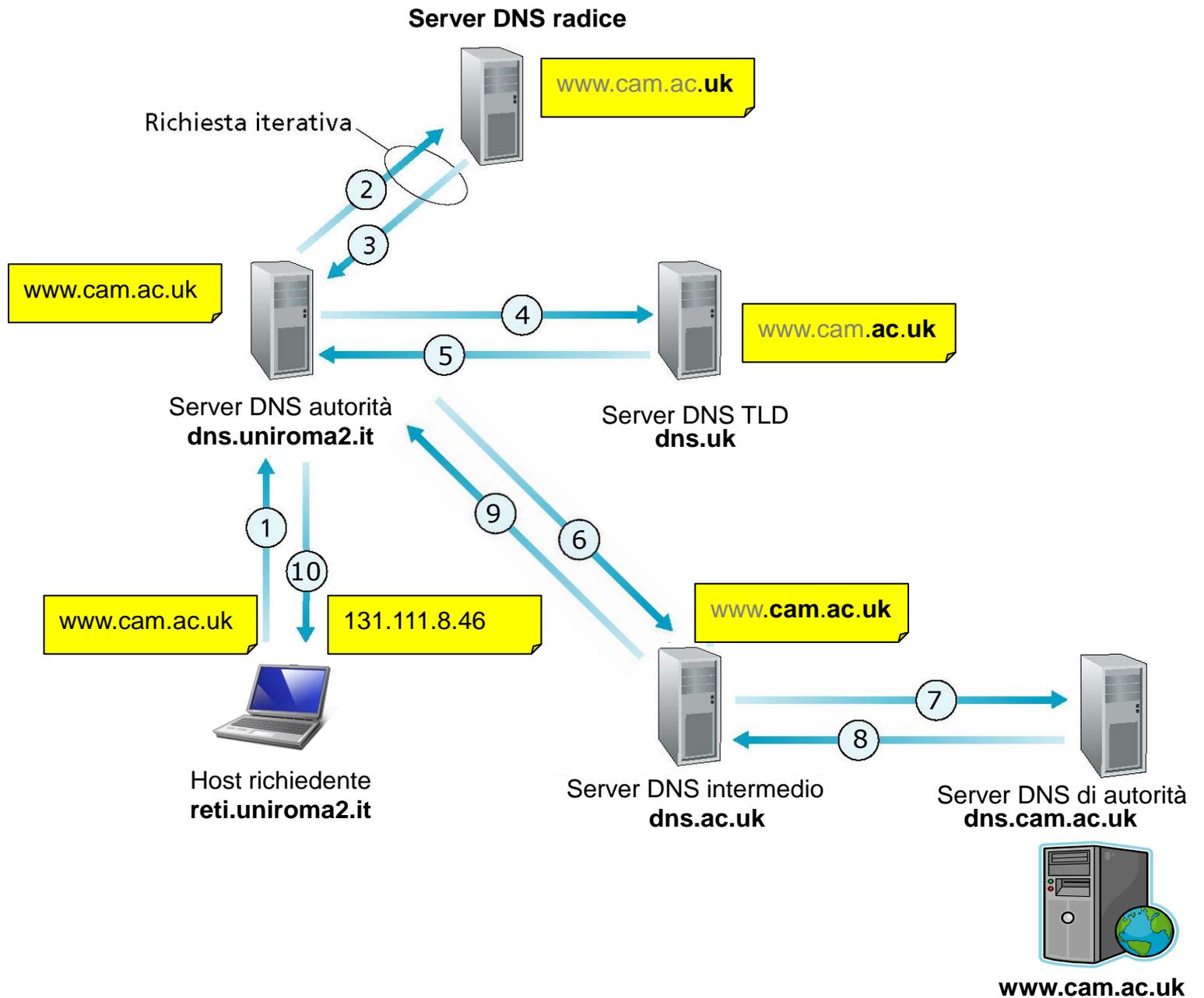
- I record MX permettono ai nomi dei server di posta di avere alias. Usando il record MX, è possibile usare lo stesso nome sia per il server di posta elettronica che per altri suoi server, come ad esempio il server Web.

- Per ottenere il nome canonico del server di posta elettronica, un client DNS deve richiedere un record di tipo **MX**; per ottenere il nome canonico dell'altro server (ad esempio il server web), il client DNS deve richiedere il record di tipo **CNAME**.
- Un name server che **è di autorità** per un host, deve contenere un **record di tipo A** per quell'host.
- Se un server **non è di autorità** per un host, allora deve contenere un **record di tipo NS** per il dominio cui l'host appartiene, e conterrà anche un record tipo A che fornisce l'indirizzo IP del server dns nel campo Valore del record NS.
- Per esempio, supponiamo che un name server **TLD it** non sia di autorità per l'host **reti.uniroma2.it**. Allora, questo name server TLD conterrà un record per il dominio cui l'host **reti.uniroma2.it** appartiene, per esempio:

**(NS, uniroma2.it, dns.uniroma2.it)**

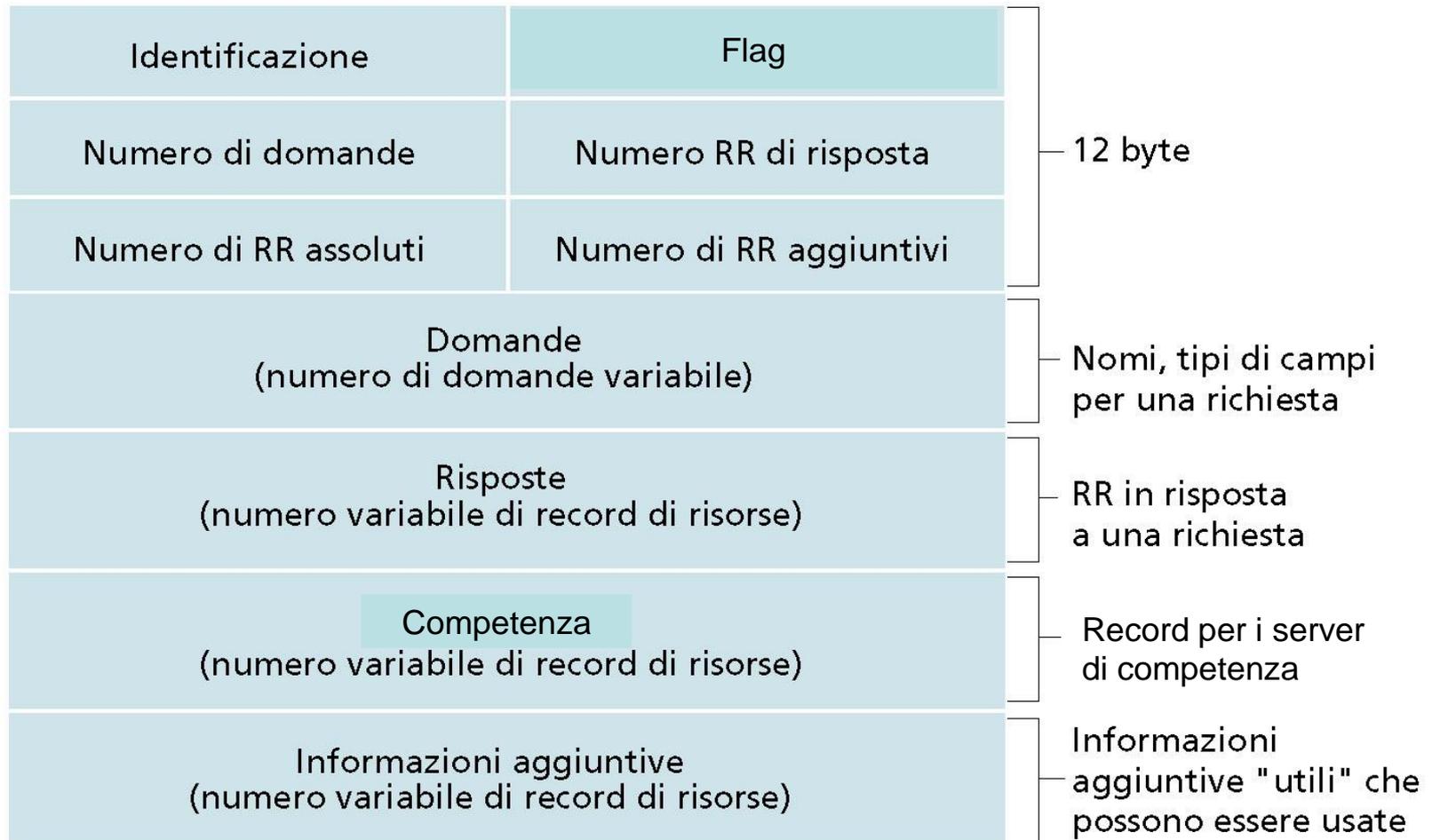
Lo stesso name server **TLD it** dovrà anche contenere un record di **tipo A**, che collega il name server **dns.uniroma2.it** all'indirizzo IP, per esempio:

**(A, dns.uniroma2.it, 160.80.1.3).**



# Messaggi DNS

- I messaggi di richiesta e di risposta del DNS hanno lo stesso formato, come illustrato nella figura.



- la **sezione dell'intestazione** è costituita dai primi 12 byte, e ha 6 campi.
  - Il campo **identificazione (16 bit)** è un numero che identifica la richiesta. Il corrispondente messaggio di risposta avrà lo stesso numero di identificazione.
  - Il campo **flag** contiene:
    - Un flag **richiesta/risposta** di un bit, vale 0 se il messaggio è una richiesta o 1 se è una risposta.
    - Un flag **autorità** di un bit, se è settato a 1 **nel messaggio di risposta** indica che un name server è un server di autorità per il nome richiesto.
    - Un flag **di richiesta di ricorsione** di un bit, viene inserito quando un client desidera che il name server effettui una ricorsione quando non trova il record.
    - Un flag **disponibilità alla ricorsione** di un bit è inserito nella risposta quando il name server supporta la ricorsione.
- Nell'intestazione ci sono anche quattro campi "**numero di**". Questi campi indicano il numero di occorrenze dei quattro tipi di sezioni di "dati" che seguono l'intestazione.

- La **sezione domande** contiene informazioni sulla richiesta che è stata fatta. Questa sezione contiene:
  - un campo **nome** che contiene il nome che verrà richiesto;
  - un campo **tipo** che indica il tipo di richiesta relativa al nome (per esempio, A, MX, CNAME,...).
- la **sezione risposte**, contiene i record di risorsa per il nome che è stato richiesto. Una risposta può contenere RR multipli, poiché un host può avere più indirizzi IP (per esempio, per server Web replicati).
- La **sezione di competenza** contiene record di altri server di competenza.
- La **sezione informazioni aggiuntive** contiene altri record aggiuntivi. Per esempio, il campo risposte in un messaggio di risposta a una richiesta MX conterrà il nome di un server di posta associato con il nome alias. La sezione aggiuntiva conterrà un record di tipo A che fornisce l'indirizzo IP per il nome canonico del server di posta.

- I dati sono inseriti nel database di un DNS sia staticamente che dinamicamente. La modalità statica, per esempio, si ottiene scrivendo i dati in un file di configurazione. La modalità di inserimento dinamico è stata aggiunta successivamente al protocollo DNS mediante un'opzione UPDATE per permettere di aggiungere o eliminare dinamicamente i dati nel database attraverso messaggi DNS.
- Il programma **nslookup**, presente sia su unix/linux che windows, consente di connettersi al name server di default e leggere i record RR.