# Livello applicazione: DNS

Gaia Maselli

# Livello di applicazione

- DNS

- Link porte TCP/UDP

http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

# DNS: Domain Name System

Identificazione degli host

- Persone: molti identificatori:
  - nome, codice fiscale,
    numero della carta d'identità
- Host Internet hanno nomi (hostname)
  - www.google.com,
  - w3.uniroma1.it
- I nomi sono facili da ricordare ma forniscono poca informazione sulla collocazione degli host all'interno di Internet
  - W3.uniroma1.it ci dice che l'host si trova probabilmente in Italia ma non dove
- Indirizzi IP per gli host:
  - indirizzo IP (32 bit) - usato per indirizzare i datagrammi
  - Corrisponde al nome usato dagli esseri umani
  - Più appropriato per le macchine

D: Come associare un indirizzo IP a un nome?

# Indirizzo IP

- Consiste di 4 byte
  - E' costituito da una stringa in cui ogni punto separa uno dei byte espressi con un numero decimale compreso tra 0 e 255
- Presenta una struttura gerarchica
  - Leggendolo da sinistra a destra otteniamo informazioni sempre più specifiche sulla collocazione dell'host in Internet (rete di appartenenza)
  - Simile ad un indirizzo postale letto dal basso verso l'alto
- Esempio
  - 121.34.230.94

# Servizio DNS

Domain Name System (RFC 1034, 1035):

- *Database distribuito* implementato in una gerarchia di *server DNS*
- *Protocollo a livello di applicazione* che consente agli host, ai router e ai server DNS di comunicare per *risolvere* i nomi (tradurre indirizzi/nomi)
  - Si noti: funzioni critiche di Internet implementate come protocollo a livello di applicazione
  - complessità nelle parti periferiche della rete
- Gira su UDP e indirizza la porta 53
- DNS viene utilizzato da altri protocolli applicativi quali HTTP, SMTP, FTP, per tradurre i nomi di host forniti dagli utenti in indirizzi IP

# Esempio di interazione con HTTP

- Un browser (ossia client HTTP) di un host utente richiede la URL `www.someschool.edu`

1. L'host fa girare il lato client dell'applicazione DNS
2. Il browser estrae il nome dell'host, `www.someschool.edu` dall'URL e lo passa al lato client dell'applicazione DNS
3. Il client DNS invia una query contenente l'hostname a un server DNS
4. Il client DNS riceve una risposta che include l'indirizzo IP corrispondente all'hostname
5. Ottenuto l'indirizzo IP dal DNS, il browser può dare inizio alla connessione TCP verso il server HTTP localizzato a quell'indirizzo IP

**N.B.**: Il DNS non interagisce direttamente con gli utenti

# Servizi DNS: aliasing

- **Host aliasing**: un host può avere uno o più sinonimi (alias)
  - Esempio: `relay1.west-coast.enterprise.com` potrebbe avere due sinonimi, quali `enterprise.com` e `www.enterprise.com`
  - `relay1.west-coast.enterprise.com` è un hostname canonico
  - I sinonimi sono più facili da ricordare
  - Il DNS può essere invocato da un'applicazione per l'hostname canonico di un sinonimo così come l'IP
- Mail server aliasing: spesso i mail server e il web server di una società hanno lo stesso alias, ma nomi canonici diversi

# Servizi DNS: distribuzione locale

- DNS viene utilizzato per distribuire il carico tra server replicati (es. web server)
- I siti con molto traffico vengono replicati su più server, e ciascuno di questi gira su un sistema terminale diverso e presenta un indirizzo IP differente
- Hostname canonico associato a un insieme di indirizzi IP
- Il DNS contiene l'insieme di indirizzi IP
- Quando un client effettua un richiesta DNS per un nome mappato in un insieme di indirizzi, il server risponde con l'insieme di indirizzi ma variando l'ordinamento a ogni risposta
- La rotazione DNS distribuisce il traffico sui server replicati

# DNS

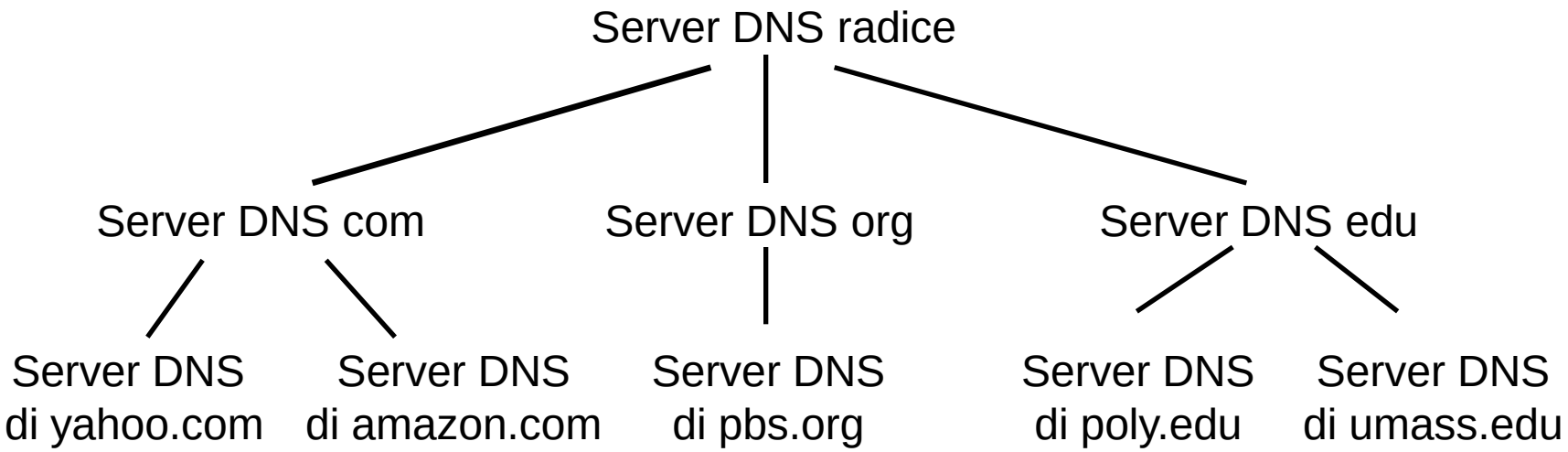
- Traduce nomi in indirizzi IP
- Ai tempi di ARPANET era un file host.txt che veniva caricato durante la notte
- Adesso è un'applicazione che gira su ogni host
- Costituita da
  - un gran numero di server DNS distribuiti per il mondo
  - Un protocollo a livello applicazione che specifica la comunicazione tra server DNS e host richiedenti

## Perché non centralizzare DNS?

- singolo punto di guasto
- volume di traffico
- database centralizzato distante
- manutenzione

Un database centralizzato su un singolo server DNS non è *scalabile* !

# Database distribuiti e gerarchici




Il client vuole l'IP di www.amazon.com; 1ª approssimazione:

- Il client interroga il server radice per trovare il server DNS com
- Il client interroga il server DNS com per ottenere il server DNS amazon.com
- Il client interroga il server DNS amazon.com per ottenere l'indirizzo IP di www.amazon.com

# DNS: server DNS radice

- contattato da un server DNS locale che non può tradurre il nome
- server DNS radice:
  - contatta un server DNS autorizzato se non conosce la mappatura
  - ottiene la mappatura
  - restituisce la mappatura al server DNS locale


13 server DNS radice nel mondo

# Server TLD e server di competenza

- Server TLD (top-level domain): si occupano dei domini com, org, net, edu, ecc. e di tutti i domini locali di alto livello, quali uk, fr, ca e jp.
  - Network Solutions gestisce i server TLD per il dominio com
  - Educause gestisce quelli per il dominio edu

- Server di competenza (*authoritative server*): ogni organizzazione dotata di host Internet pubblicamente accessibili (quali i server web e i server di posta) deve fornire i record DNS di pubblico dominio che mappano i nomi di tali host in indirizzi IP.
  - possono essere mantenuti dall'organizzazione o dal service provider

# Server DNS locale

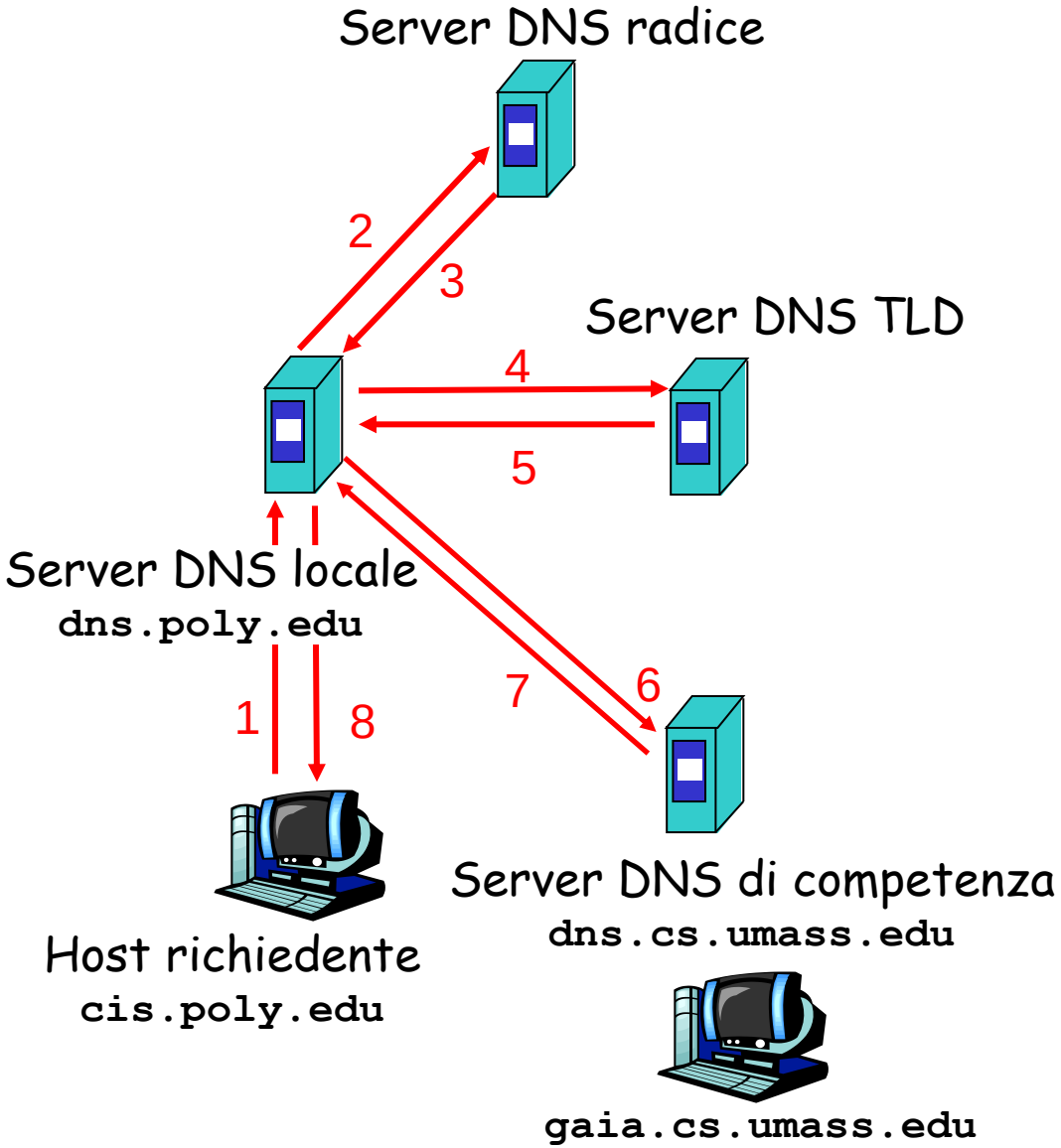
- Non appartiene strettamente alla gerarchia dei server
- Ciascun ISP (università, società, ISP residenziale) ha un server DNS locale.
  - detto anche "default name server"
- Quando un host effettua una richiesta DNS, la query viene inviata al suo server DNS locale
  - il server DNS locale opera da proxy e inoltra la query in una gerarchia di server DNS

# Esempio

- L'host cis.poly.edu vuole l'indirizzo IP di gaia.cs.umass.edu

Query iterativa: (2-7)

- Il server contattato risponde con il nome del server da contattare
- "Io non conosco questo nome, ma puoi chiederlo a questo server".

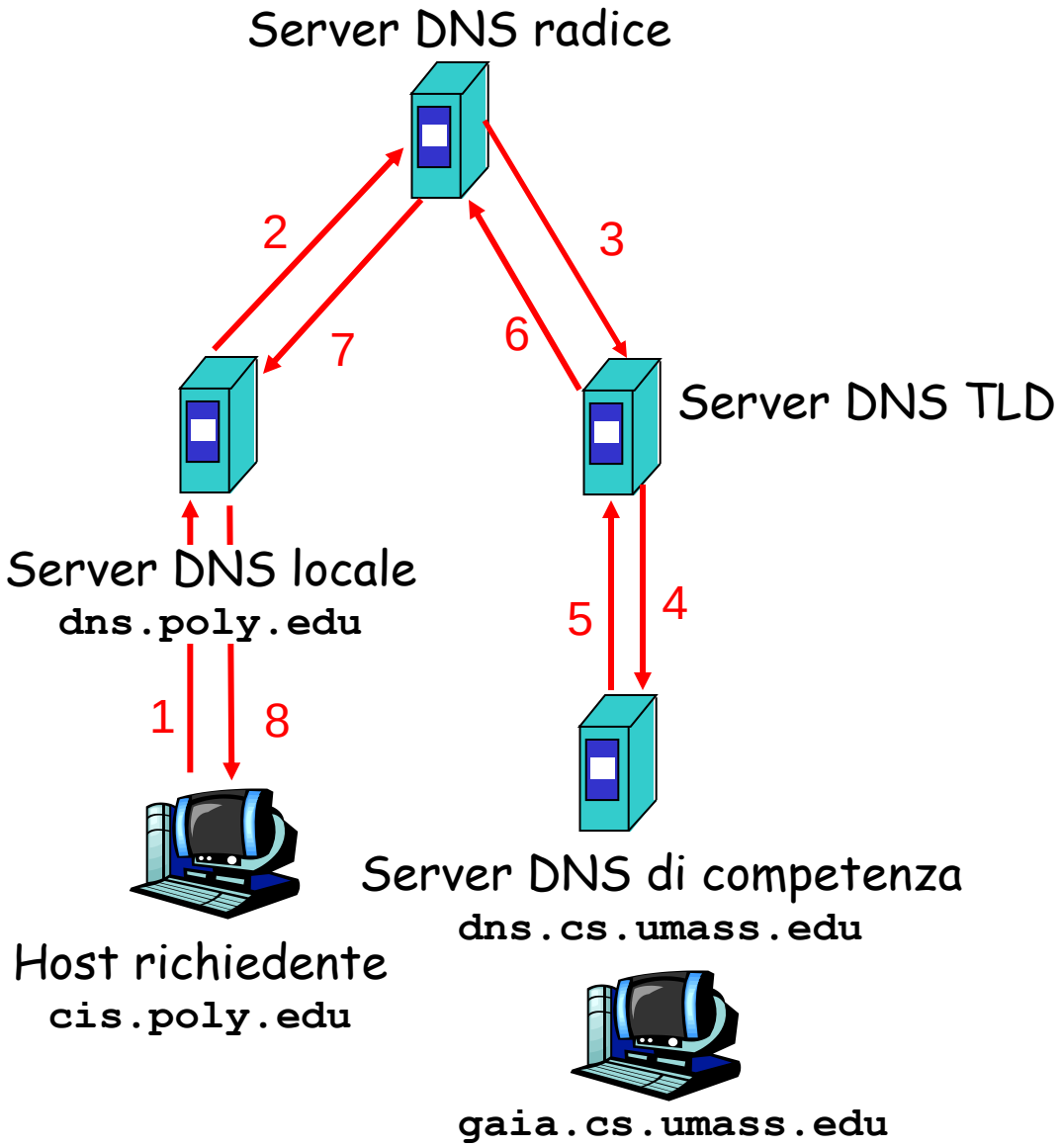



N.B. Per ottenere la mappatura di un hostname sono stai inviati 8 messaggi !!!

# Esempio

## Query ricorsiva:

- Affida il compito di tradurre il nome al server DNS contattato



# DNS: caching e aggiornamento dei record

- DNS sfrutta il caching per migliorare le prestazioni di ritardo e per ridurre il numero di messaggi DNS che "rimbalzano" in Internet
- Una volta che un server DNS impara la mappatura, la mette nella *cache*
  - le informazioni nella cache vengono invalidate (spariscono) dopo un certo periodo di tempo (es. 2 giorni)
  - tipicamente un server DNS locale memorizza nella cache gli indirizzi IP dei server TLD (ma anche quelli di competenza)
    - quindi i server DNS radice non vengono visitati spesso
- Esempio: più utenti in dipartimento che si connettono sul sito del Corriere
- I meccanismi di aggiornamento/notifica sono progettati da IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

# Record DNS

DNS: database distribuito che memorizza i record di risorsa o resource record (RR). Ogni messaggio di risposta DNS trasporta uno o più RR

Formato RR: **(Name, Value, Type, TTL)**

Tempo residuo di vita

- Type=A
  - **name** è il nome dell'host
  - **value** è l'indirizzo IP

Es. (`relay1.bar.foo.com`, 45.37.93.126, A)

- Type=NS
  - **name** è il dominio (ad esempio foo.com)
  - **value** è il nome dell'host del server di competenza di questo dominio

Es. (`foo.com`, `dns.foo.com`, NS)

- Type=CNAME
  - **name** è il nome alias di qualche nome "canonico" (nome vero)
  - **value** è il nome canonico

Es. (`foo.com`, `relay1.bar.foo.com`, CNAME)

- Type=MX
  - **value** è il nome canonico del server di posta associato a **name**

Es. (`foo.com`, `mail.bar.foo.com`, MX)

# Esempio

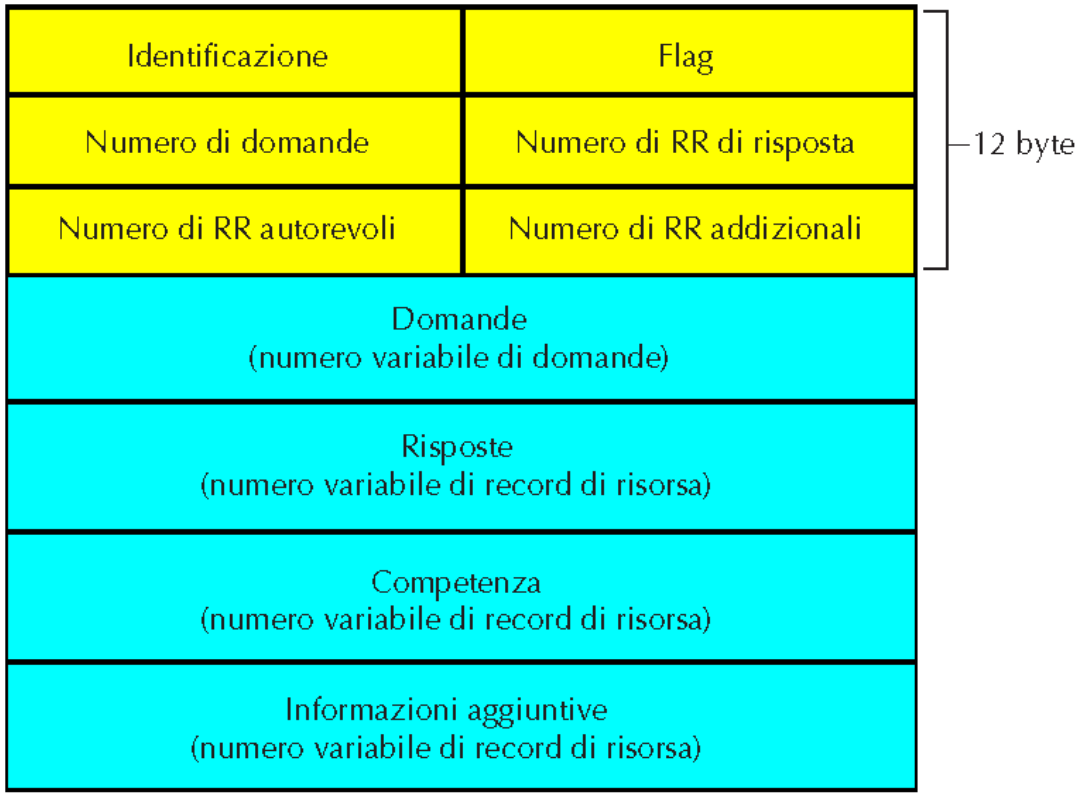
- Server di competenza per un hostname
  - Contiene un record di tipo A per l'hostname
  - Es. (`corsi.di.uniroma1.it, 131.111.45.68, A`)
- Server non di competenza per un dato hostname
  - Contiene un record di tipo NS per il dominio che include l'hostname
  - Contiene un record di tipo A che fornisce l'indirizzo IP del server DNS nel campo `value` del record NS
- Es.:
  - Un server TLD it non è competente per l'host `corsi.di.uniroma1.it`
  - Contiene (`uniroma1.it, dns.uniroma1.it, NS`)
    (`dns.uniroma1.it, 128.119.40.111, A`)

# Messaggi DNS

Protocollo DNS: domande (query) e messaggi di *risposta*, entrambi con lo stesso *formato*

Intestazione del messaggio

- Identificazione: numero di 16 bit per la domanda; la risposta alla domanda usa lo stesso numero
- Flag:
  - domanda o risposta
  - richiesta di ricorsione
  - ricorsione disponibile
  - risposta di competenza (il server è competente per il nome richiesto)
- Numero di: numero di occorrenze delle quattro sezioni di tipo dati che seguono



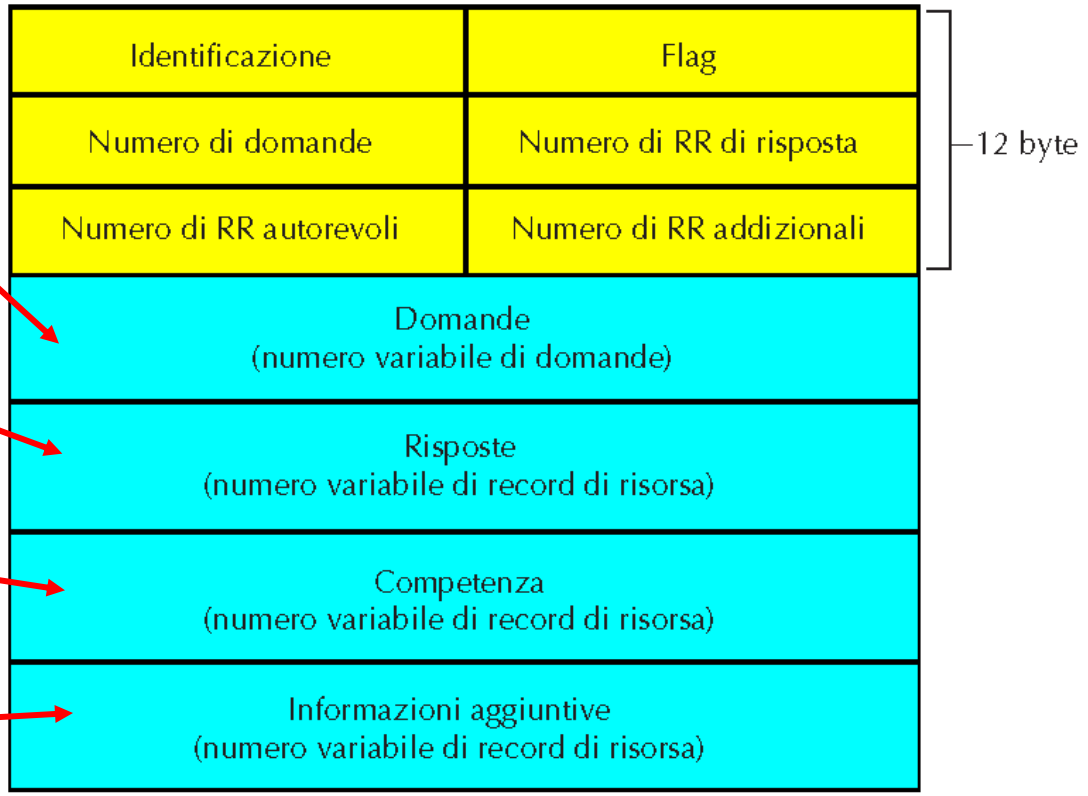
# Messaggi DNS

Campi per il nome richiesto e il tipo di domanda (A, MX)

RR nella risposta alla domanda
Più RR nel caso di p.e. di server replicati

Record per i server di competenza

Informazioni extra che possono essere usate




Nel caso di una risposta MX, il campo di risposta contiene il record MX con il nome canonico del server di posta, mentre la sezione aggiuntiva contiene un record di tipo A con l'indirizzo IP relativo all'hostname canonico del server di posta

→ Provare con nslookup

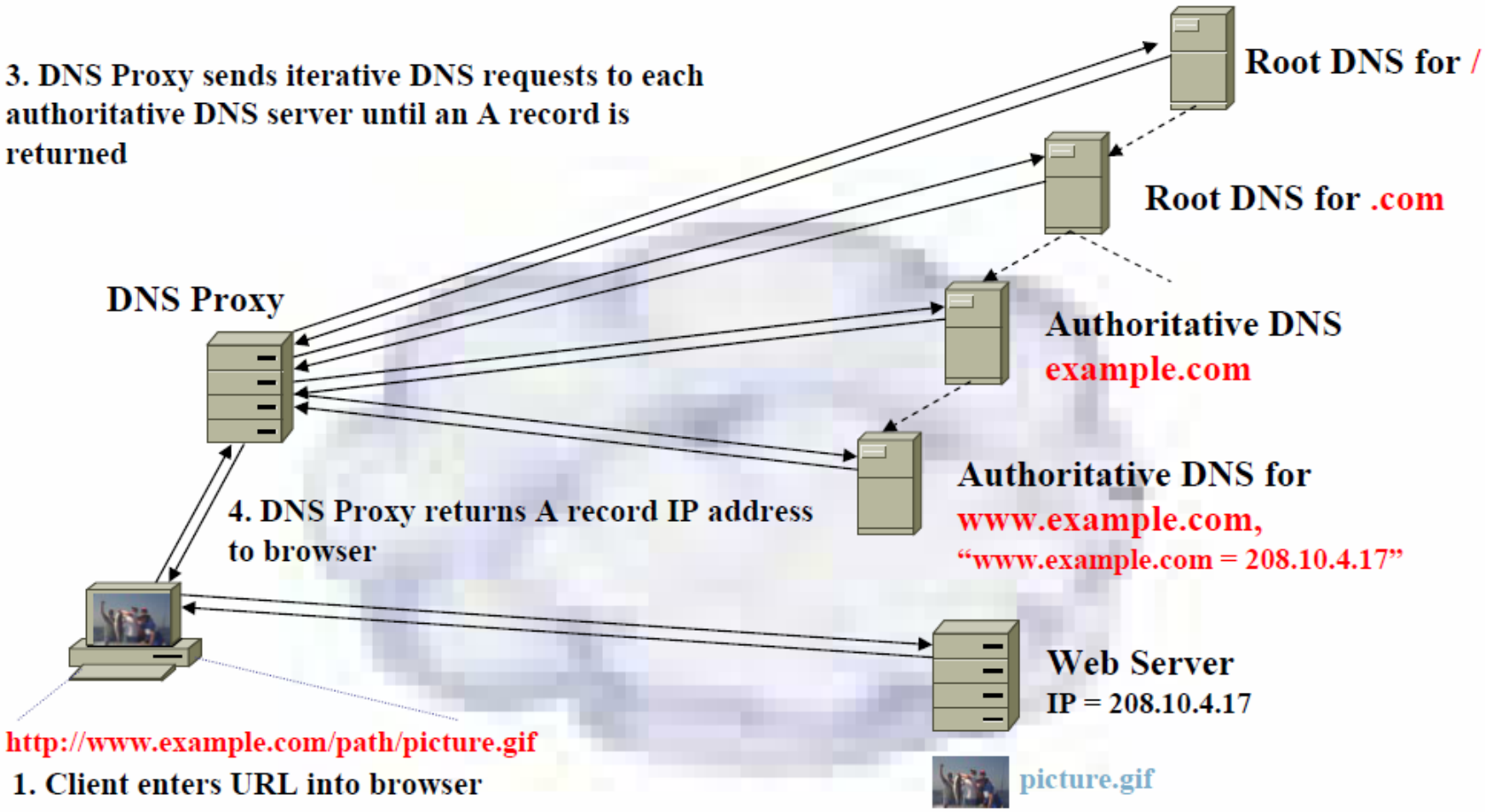
# Inserire record nel database DNS

- Esempio: abbiamo appena avviato la nuova società "Network Utopia"
- Registriamo il nome **networkuptopia.com** presso registrar (ad esempio, Network Solutions)
  - Forniamo a registrar i nomi e gli indirizzi IP dei server DNS di competenza (primario e secondario)
  - Registrar inserisce due RR nel server TLD com:

  - (networkutopia.com, dns1.networkutopia.com, NS)
  - (dns1.networkutopia.com, 212.212.212.1, A)

- Inseriamo nel server di competenza un record tipo A per www.networkuptopia.com e un record tipo MX per networkutopia.com
- In che modo gli utenti otterranno l'indirizzo IP del nostro sito web?

# Esempio


3. DNS Proxy sends iterative DNS requests to each authoritative DNS server until an A record is returned
Root DNS for /
Root DNS for .com
DNS Proxy
Authoritative DNS example.com
Authoritative DNS for www.example.com, "www.example.com = 208.10.4.17"
4. DNS Proxy returns A record IP address to browser
Web Server IP = 208.10.4.17
http://www.example.com/path/picture.gif
picture.gif
1. Client enters URL into browser
2. Browser sends recursive DNS request for www.example.com to DNS Proxy
5. Browser makes HTTP request to 208.10.4.17 for "picture.gif"