

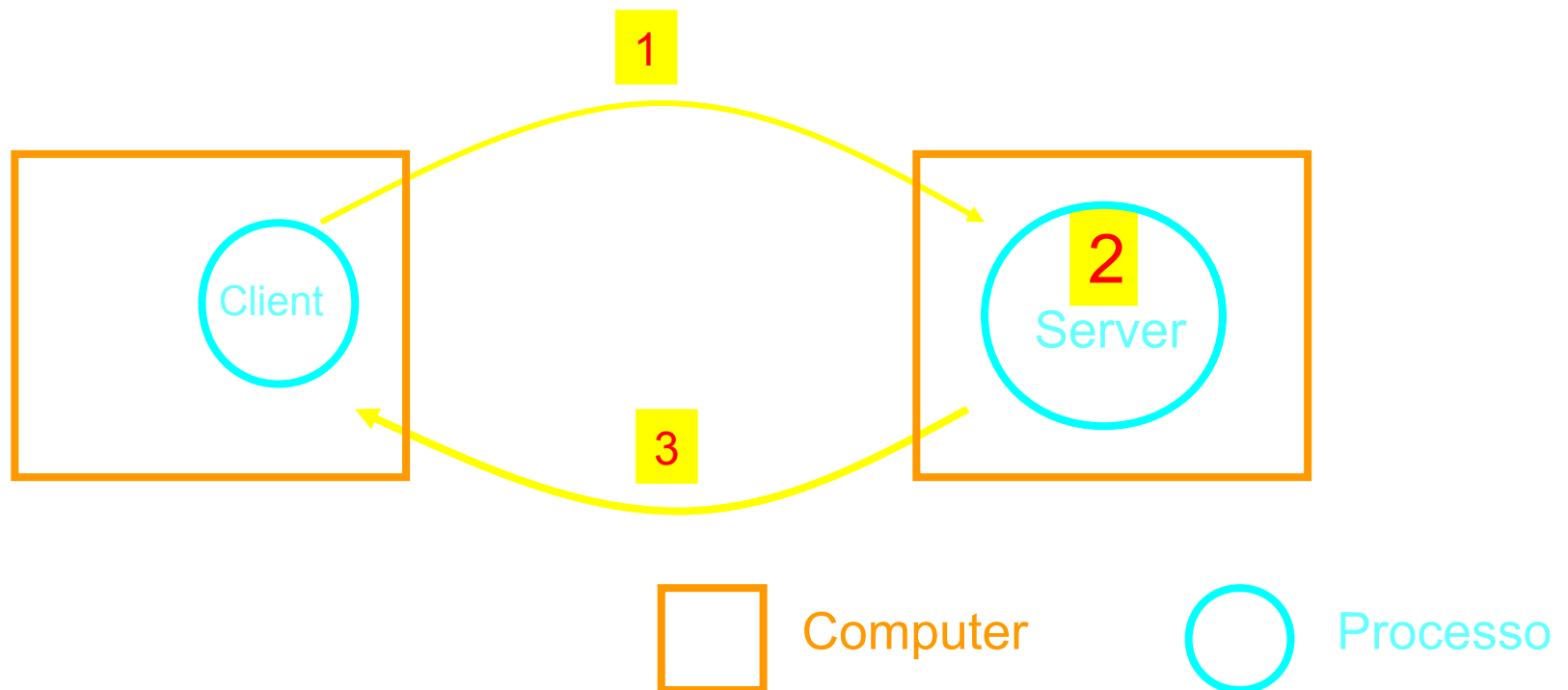
# **PARTE 7**

# **DOMAIN NAME SYSTEM (DNS)**

- **Un'applicazione Internet al servizio delle applicazioni Internet**
- **Un esempio di sistema distribuito geograficamente che funziona molto bene**
- **Introduce un altro livello di naming in Internet, oltre gli indirizzi IP, che risulta "più vicino all'utente" (ma non solo per questo ...)**

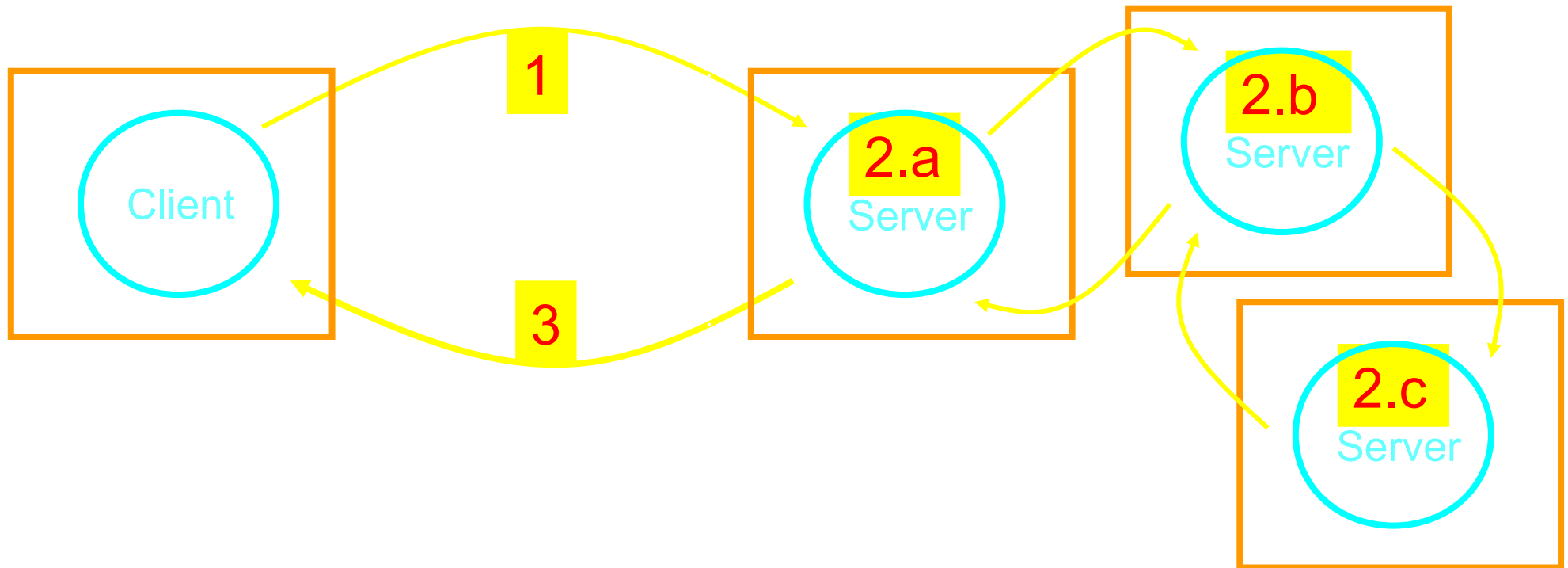
# Servizi Internet: Modello client-server

1. Trasmissione di una richiesta dal processo client al processo server (*request*)
2. Elaborazione della richiesta da parte del server
3. Trasmissione di una risposta al client (*reply*)



# Modello client-server (servizio fornito da server multipli)

1. Trasmissione di una richiesta dal processo client al processo server
2. Elaborazione della richiesta da parte del server con invocazione di elaborazioni da parte di uno o più processi
3. Trasmissione di una risposta al client



## **Modulo 1: Identificatori degli host**

# ***“Identificatori” in Internet***

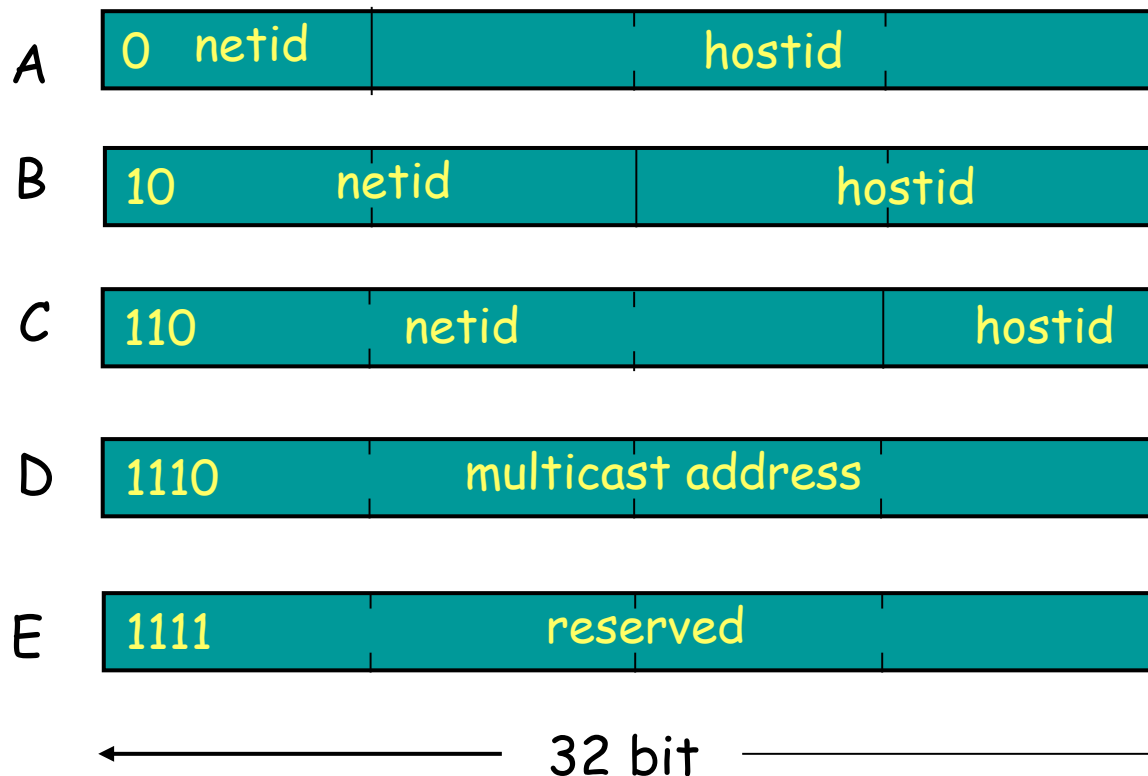
- **Le persone hanno molteplici “identificatori”: nome, n° passaporto, codice fiscale, ...**
- **I telefoni sono denotati da un unico numero**
- **Tutti i dispositivi collegati ad Internet (host, router) hanno almeno due identificatori:**
  - Indirizzo IP (numero di 32 bit): utilizzato per indirizzare ed instradare i pacchetti nella rete
  - Hostname (stringa alfanumerica di al più 255 caratteri): nome logico utilizzato dalle persone

# Oltre agli indirizzi IP, ci sono ...

## 5 classi di indirizzi IP:

*classe A, classe B, classe C, classe D, classe E*

Classe



## ... gli hostname

- Sequenza di label separate da punti
- Ogni label si compone di al più 63 caratteri alfanumerici
- L'intero hostname può essere di al più 255 caratteri

- 

### Esempi

- w3c.org
- samba.ing.unimo.it
- www.unimo.it
- promo.dim.ing.unimo.it

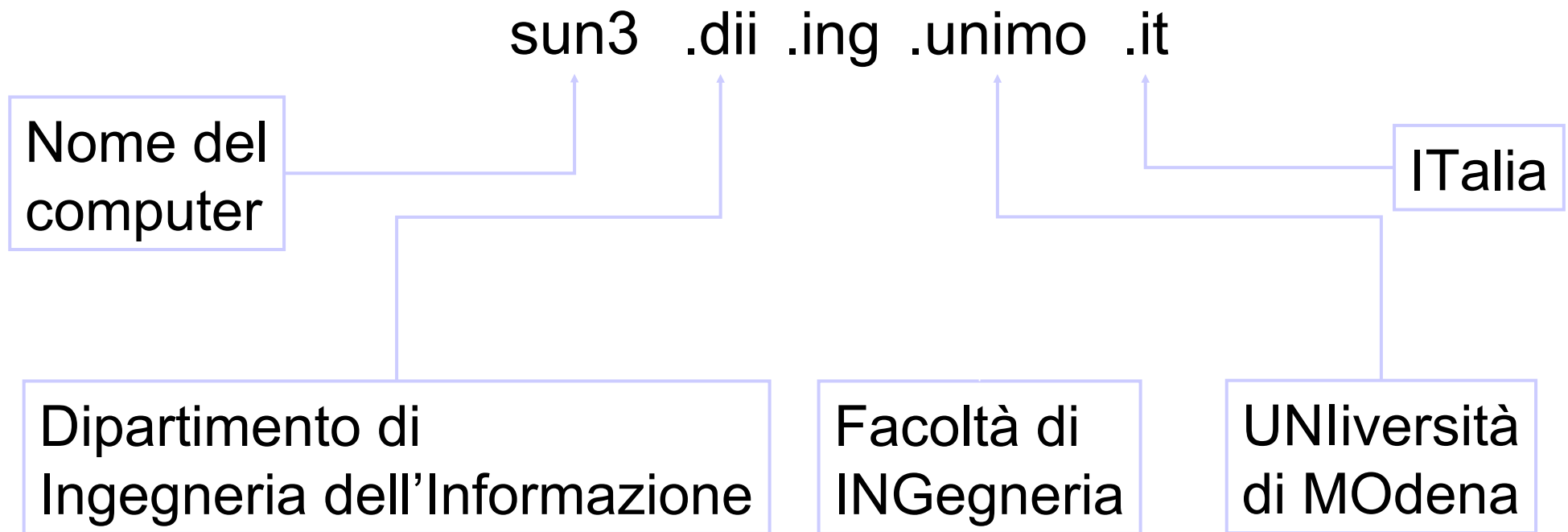
Non c'è alcuna corrispondenza tra le label dell'hostname ed i quattro campi dell'indirizzo IP



# Hostname (canonico)

- **Dato lo scopo rivolto verso l'utente, all'hostname si preferiscono attribuire valori mnemonici.**

**Es.: nome del computer e dominio di appartenenza:**



# *Vantaggi degli hostname*

- **Gli hostname favoriscono l'usabilità delle applicazioni Internet consentendo agli utenti di far riferimento a nomi mnemonici e gerarchici invece che a indirizzi IP numerici**
- **Servono anche ad altro?**

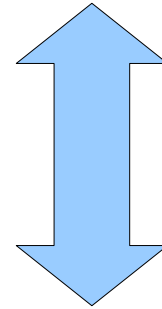
# Altre motivazioni oltre l'usabilità

- **Specificare l'indirizzo di un host con un valore costante renderebbe l'interazione client/server più veloce, ma:**
  - il software del client dovrebbe essere ricompilato ogni volta che il server venisse spostato
  - il client non potrebbe usare più di un server
- **L'hostname è un buon compromesso che consente:**
  - il collegamento (*binding*) tra hostname e indirizzo IP fino a tempo di esecuzione
  - l'uso di alias per un hostname

Tipico compromesso: maggiore flessibilità a costo di perdita di efficienza

## *2 meccanismi di naming → necessità di traduzione*

Hostname: sun3.dii.ing.unimo.it



Indirizzo IP: 134.56.26.68

*(10000110.00111000.00011010.01000100)*

# **Traduzione hostname→indirizzo IP (e viceversa)**

- **Se la rete ha pochi nodi: soluzione centralizzata con uno spazio piatto dei nomi**

**Per es.,**

- inizialmente il database centralizzato del NIC
- file hosts.txt
- **Se la rete ha milioni di nodi: soluzione distribuita con uno spazio gerarchico dei nomi**
  - Domain Name System (DNS), operativo dal 1985

# *Domain Name System (DNS)*

- **Realizza uno spazio dei nomi gerarchico e permette la traduzione del nome mnemonico di un host in un indirizzo IP e viceversa**
- **Implementa un meccanismo efficiente per “risolvere” un hostname in un indirizzo IP e viceversa**
  - mediante multipli name server
  - server distribuiti su scala geografica
  - deleghe multiple
  - uso di caching
  - uso di protocollo di trasporto “veloce” (UDP)

## **Modulo 2: Organizzazione logica dello spazio dei nomi**

# *What's in a name?*

- **Tutto!**
- **Importanza del brand per qualsiasi azienda, ente, organizzazione**
- **Il brand su Internet è dato dall'hostname**
- **Basta pensare all'effetto delle dotcom**
  - google.com
  - ebay.com
  - amazon.com
  - ...



# *Domini di massimo livello*

## *Top Level Domain (TLD)*

- **gTLD: generic TLD**
  - .com
  - .edu
  - .org
  - ...
- **ccTLD: country code TLD**
  - .uk
  - .fr
  - .it
  - ...
- **iTLD: infrastructure TLD**
  - .arpa

# Domini Top level storici

Nome del dominio	Significato
com	Organizzazioni commerciali
edu	Istituzioni Usa per l'istruzione
gov	Istituzioni governative USA
mil	Istituzioni militari USA
net	Centri di supporto per la rete
org	Organizzazioni senza scopo di lucro
arpa	Dominio della rete Arpanet
int	Organizzazioni internazionali
Codici nazionali (it, uk, us, fr, es, ...)	ccTLD

Caso interessante: Tonga e Tuvalu

# *I nuovi TLD*

- **Sono stati approvati i seguenti nuovi Top Level Domain (i primi tre attivi da gennaio 2002)**
- **Unsponsored TLD (uTLD)**
  - .biz (www.NIC.biz)
  - .info (www.NIC.info)
  - .name (www.NIC.name)
  - .eu (europe) - ATTIVO DAL 2006
  - ...

# *I nuovi TLD*

- **Sponsored TLD (sTLD)**

- .museum
- .coop
- .aero
- ...

## **Generic TLD (gTLD) liberalizzati nel 2012**

### **Elenco TLD attivi:**

**<http://data.iana.org/TLD/tlds-alpha-by-domain.txt>**

# ***Second-Level Domain (SLD)***

- **Corrispondono ai veri brand di un'organizzazione**
- **I più importanti servizi Internet (WWW e email) si basano fortemente sulla semplicità del mezzo comunicativo**
  - Se penso al sito Web della IBM Inc., provo subito: `www.ibm.com` o addirittura `ibm.com`
  - Se devo spedire una mail a Riccardo Lancellotti della Università di Modena, penso a `riccardo.lancellotti@unimore.it`

# *Second-Level Domain (SLD)*

- **I nomi hanno un valore economico perché sono associati con i beni/servizi prodotti e con la reputazione della organizzazione**
  - Gran parte del valore della società Amazon è dato dal suo nome di dominio Amazon.com
  - Perdere la registrazione del dominio è un danno economico importante (es. mediaset.com)

# *Conseguenze del valore*

- **Inizio del commercio dei nomi**
- **Registrazione di nomi facili da ricordare e che conducono ad una categoria di prodotti/servizi. Es., car.com,**
- **Cybersquatting: registrare un dominio che contiene il brand di un'azienda e provare a rivenderlo**
  - es.: ferrari.it

# *Conseguenze del valore*

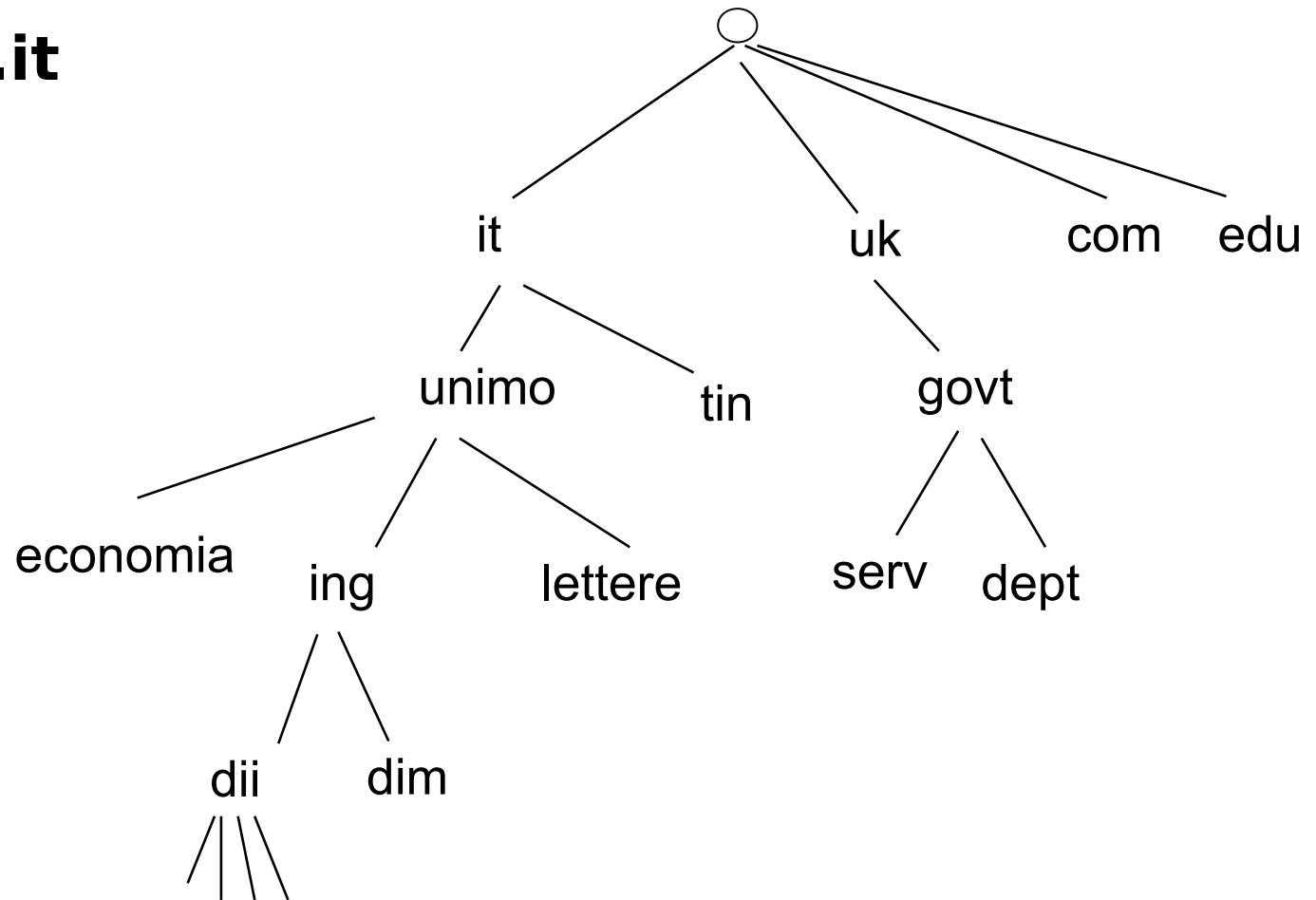
- **Il cybersquatting porta all'adozione di regole come l'Anticybersquatting Consumer Protection Act (ACPA) e un sistema di politiche di arbitrato incluse le Uniform Dispute Resolution Policy (UDRP) dell'ICANN**  
**<http://www.icann.org/udrp/>**



# Organizzazione gerarchica dei domini

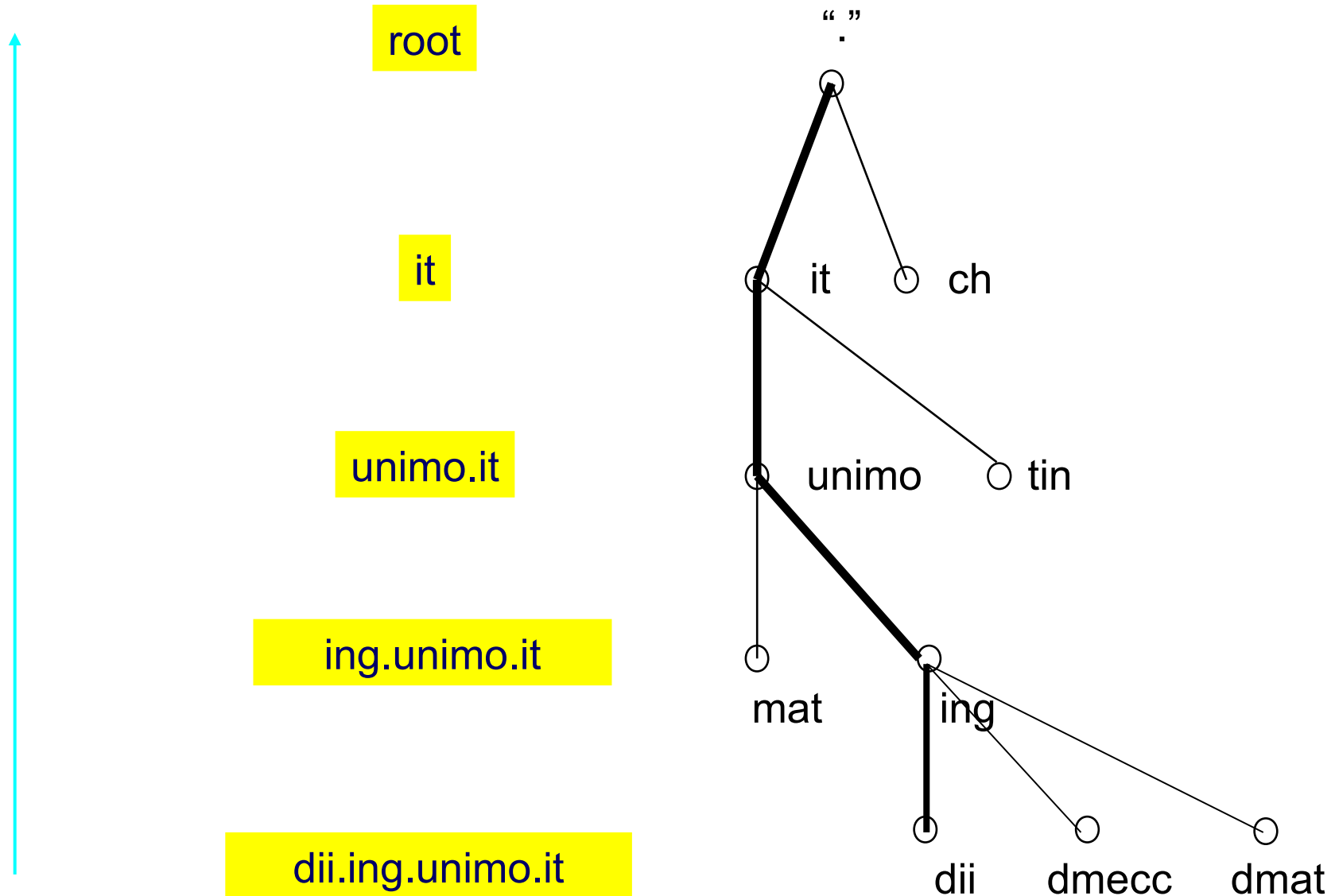
- **dii.ing.unimo.it**
- **dept.govt.uk**

*La stringa relativa ad un host non ha limiti nel numero di campi*



Esempio: Università di Modena “unimo”, con tre Facoltà (“economia”, “lettere”, “ing”), quest’ultima con due dipartimenti Informazione (“dii”) e Meccanica (“dim”), nel primo dei quali sono registrati diversi host

# Organizzazione gerarchica: altro esempio



## **Modulo 3: Componenti del DNS**

# *Obiettivi progettuali del DNS*

- **Spazio dei nomi consistente**
- **Sistema con elevata tolleranza ai guasti**
  - Nessun “single point of failure”
- **Sistema scalabile**
  - Partizionamento del database dei nomi
  - Organizzazione distribuita con possibilità di caching dell’informazione in più punti
  - Decentralizzazione del meccanismo di registrazione degli indirizzi
- **Sistema funzionante in reti eterogenee**
  - soggette a diverse amministrazioni che possono avere differenti politiche di gestione
  - indipendente dal sistema di comunicazione, dai protocolli utilizzati e dal tipo di piattaforme sottostanti

# Componenti del DNS - INDICE

- Zone e Name Servers

→ Ovvero i possessori e gestori dell'informazione, con le funzionalità di server abilitati a rispondere alle query dei client e di altri server

- **Domain Name Space e Resource Records**

→ Ovvero i dati su zone, descrittori, informazioni

- **Resolvers**

→ Ovvero i (primi) client del sistema DNS che sottomettono query per informazioni su hostname e indirizzi IP per conto delle applicazioni Internet



# Organizzazione gerarchica dei domini

Root level



TLD

COM

NET

ORG

SLD

CIK

FOOD

LASER

IEEE

PPT

MAIL

WWW

WWW

WWW

WWW

TECH

MAIL

Webmail

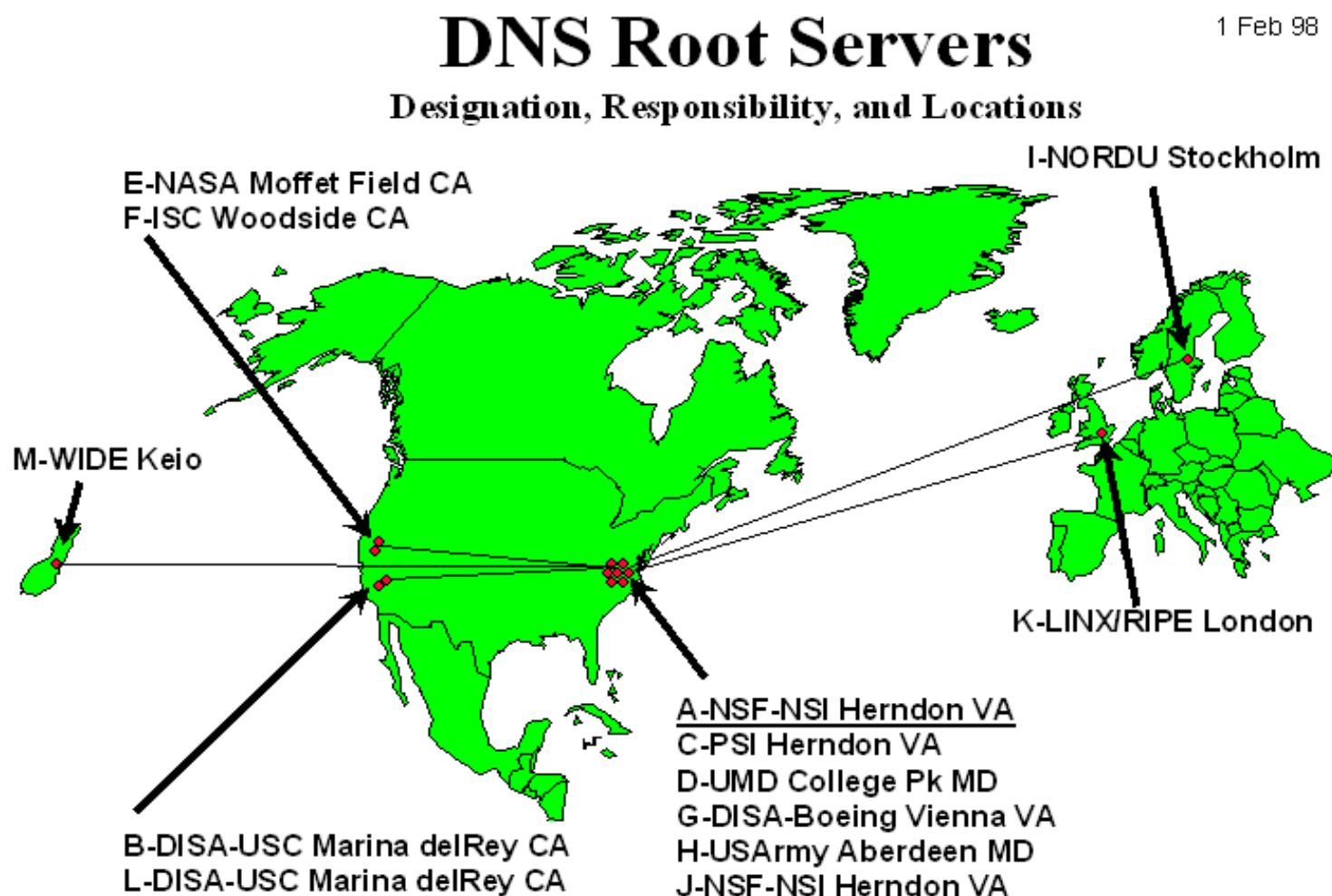
RESEARCH

PERSONAL

# *Classi di name server*

- **Root name server (.) – la radice dell'albero dei domini**
- **TLD name server (relativi ai domini top-level:  
                                  .com, .edu, .org, .it, .uk, ...)**
- **SLD name server**
- **Local name server (non appartiene a una gerarchia come i precedenti; ogni ISP e organizzazione gestisce uno o più name server locali: sono le foglie dell'albero)**

# I 13 Root name server (fino al 2004)



A: root name server primario che ha la copia ufficiale della Zona Root  
B-M: root name server secondari (ricevono aggiornamenti ogni 12 ore)



# ***Nuova organizzazione dei root name server***

<b><u>Nome</u></b>	<b><u>Organizzazione</u></b>	<b><u>Luogo</u></b>	<b><u>URL</u></b>
<b>A</b>	<b>Network Solutions, Inc</b>	<b>Herndon, VA, USA</b>	<b><a href="http://www.netsol.com">http://www.netsol.com</a></b>
<b>B</b>	<b>Information Sciences Institute</b>		
	<b>University of Southern California</b>	<b>Marina Del Rey, CA, USA</b>	<b><a href="http://www.isi.edu">http://www.isi.edu</a></b>
<b>C</b>	<b>PSINet</b>	<b>Herndon, VA, USA</b>	<b><a href="http://www.psi.net">http://www.psi.net</a></b>
<b>D</b>	<b>University of Maryland</b>	<b>College Park, MD, USA</b>	<b><a href="http://www.umd.edu">http://www.umd.edu</a></b>
<b>E</b>	<b>NASA</b>	<b>Mountain View, CA, USA</b>	<b><a href="http://www.nasa.gov">http://www.nasa.gov</a></b>
<b>F</b>	<b>Internet Software Consortium</b>	<b>Palo Alto, CA, USA</b>	<b><a href="http://www.isc.org">http://www.isc.org</a></b>
<b>G</b>	<b>Defense Inform. Systems Agency</b>	<b>Vienna, VA, USA</b>	<b><a href="http://nic.mil">http://nic.mil</a></b>
<b>H</b>	<b>Army Research Laboratory</b>	<b>Aberdeen, MD, USA</b>	<b><a href="http://www.arl.mil">http://www.arl.mil</a></b>
<b>I</b>	<b>NORDUNet</b>	<b>Stockholm, Sweden</b>	<b><a href="http://www.nordu.net">http://www.nordu.net</a></b>
<b>J</b>	<b>(TBD)</b>	<b>Herndon, VA, USA</b>	<b>N/A</b>
<b>K</b>	<b>RIPE-NCC</b>	<b>London, UK</b>	<b><a href="http://www.ripe.net">http://www.ripe.net</a></b>
<b>L</b>	<b>(TBD)</b>	<b>Marina Del Rey, CA</b>	<b>USA N/A</b>
<b>M</b>	<b>WIDE</b>	<b>Tokyo, Japan</b>	<b><a href="http://www.wide.ad.jp">http://www.wide.ad.jp</a></b>
<b>Z</b>	<b>- sostituto di A</b>		

# *Piattaforme dei root name server*

- **I root name server sono i computer che forniscono accesso al file della “root zone” per le necessarie operazioni di DNS resolution**
- **A causa dei limiti del protocollo UDP utilizzato dal DNS, il numero di macchine è limitato a 13 (il pacchetto UDP deve poter contenere tutti i nomi dei server), sebbene sia stato trovato un “trucco” per rimuovere il problema → anycast**

# *Piattaforme dei root name server*

- **Dopo lunghi dibattiti, si è arrivati a diversificare l'amministrazione dei 13 root name server, che attualmente sono gestiti da enti militari statunitensi, organizzazioni commerciali e non-profit, Internet service provider, università, e istituti di ricerca. In particolare, 3 dei 13 server sono localizzati al di fuori degli Stati Uniti (uno a Londra, ma amministrato dall'Olanda, uno in Giappone, uno in Svezia)**

# ***Piattaforme dei root name server (cont.)***

- **Tutti e 13 i name server sono posti in ambienti controllati e protetti anche da contingenze ambientali, che includono limitazioni e controlli sugli accessi fisici, protezioni contro incendi, allagamenti, e black-out (con generatori autonomi), diverse connessioni ad Internet (dal livello 1 al livello 3)**
- **I root name server B-M sono costituiti da più macchine, anche se ciascun name server è “logicamente uno”**
- **Il root name server A è fisicamente costituito da una macchina, anche se in caso di emergenza le sue funzionalità possono essere rimpiazzate dal server Z**

## ***Piattaforme dei root name server (cont.)***

- **Tutti i root name server utilizzano qualche variante del sistema operativo Unix (assolutamente non Windows...!). Tuttavia, sia l'hardware sia il sistema operativo su cui si basano i name server è estremamente eterogeneo: tra i 13 name server, si contano 7 diverse piattaforme hardware con 8 diverse versioni di sistema operativo forniti da 5 diversi vendor**
- **“Internet continuerà a funzionare, anche se 2/3 dei root name server dovessero risultare irraggiungibili” (RFC-2870)**

# *Situazione attuale*

- **A – Verisign, Dulles, Virginia, USA**
- **B – Information Sciences Institute, Marina del Rey, California, USA**
- **C – Cogent (top 10 provider), distribuito in anycast**
- **D – University of Maryland, College Park, Maryland, USA**
- **E – NASA, Mountain View, California, USA**
- **F – Internet Software Consortium, distribuito in anycast**
- **G – NIC del DoD, Vienna, Virginia, USA**
- **H – U.S. Army Research Lab, Poligono di Aberdeen, Maryland, USA**
- **I – Autonomica/NORDUnet (Svezia), distribuito in anycast**
- **J – VeriSign, distribuito in anycast**
- **K – RIPE NCC (Europa), distribuito in anycast**
- **L – ICANN, Los Angeles, California, USA**
- **M – WIDE Project (Japan), distribuito in anycast**

# Indirizzo anycast

- **E' un indirizzo IP associato a indirizzi IP di più host**
  - **Nel momento in cui un pacchetto è diretto ad un indirizzo anycast, verrà recapitato ad uno qualsiasi degli indirizzi IP associati all'indirizzo**
  - **La risposta si ottiene dal primo host che viene raggiunto (tipicamente, il più vicino). Vantaggi:**
    - Si riduce il tempo di risposta
    - Si distribuisce il carico tra più name server
    - Si aumenta l'affidabilità
- Scelta molto valida per il servizio DNS**

# La situazione attuale





# *Funzionamento dei Root name server*

## **File della “root zone”**

- **Attualmente, questo file è gestito dall'ente Network Solutions Incorporated of Herndon, Virginia (USA) ed è reso disponibile ai 12 root name server secondari dal server primario a.root-servers.net**
- **Il controllo sui cambiamenti in questo file è di competenza di ICANN. I cambiamenti, tipicamente modifiche dei name server che gestiscono i top level domains, sono effettuati uno, due volte a settimana**

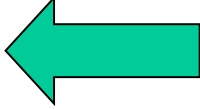
# *Funzionamento dei Root name server*

- **Il file della “root zone” è trasmesso ai root name server**
  - in modalità in-band mediante il protocollo DNS (“zone transfer” come descritto in RFC 1034)
  - in modalità out-of-band mediante il protocollo FTP (come descritto in RFC 952)
- **Data la dimensione relativamente piccola del file della “root zone”, la maggior parte degli aggiornamenti sono propagati mediante “DNS zone transfers”**

# *TLD name server*

- **Gestiscono i dati e le richieste relativamente ai gTLD e ai ccTLD:**
  - .net
  - .com
  - .org
  - ...
  - .it
  - .uk
  - .eu
  - ...
- **Devono registrarsi presso i root name server**

# *Classi di name server – i più visibili*

- **SLD name server** 
- **Local name server**
  - (ogni ISP e organizzazione gestisce uno o più name server locali: sono le foglie dell'albero)

# Principio di delega del DNS

- **Ciascuna organizzazione che possiede e gestisce un nome a dominio (“contratto diretto”) è responsabile dell’operatività di almeno un authoritative name server che:**
  - deve essere registrato presso il dominio gerarchicamente superiore (es., SLD →TLD)
  - deve fornire la corrispondenza tra tutti gli hostname del dominio ed i rispettivi indirizzi IP

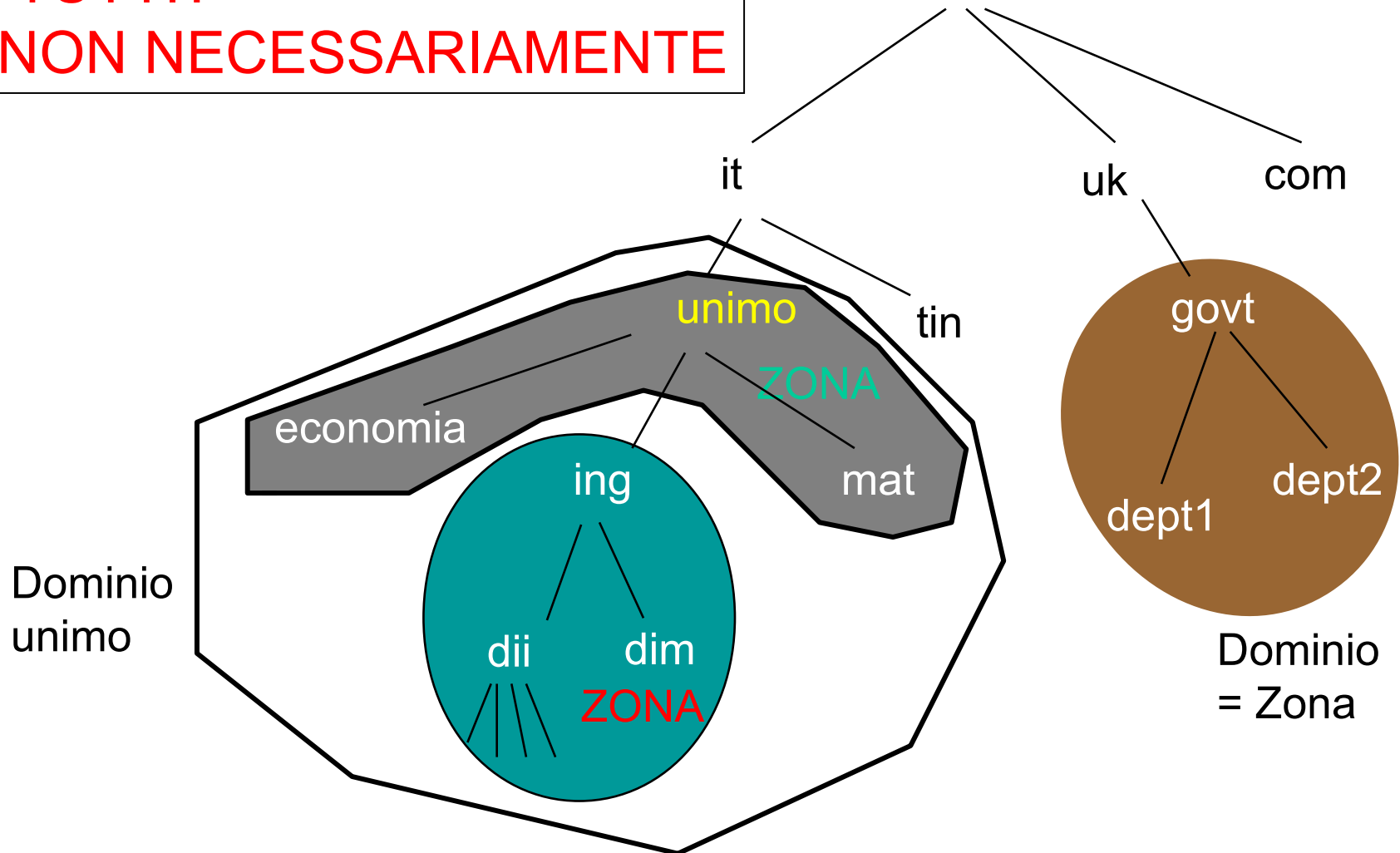
## **Esempio:**

- Qualche name server gestito dall’organizzazione UNIMO è responsabile degli hostname in unimo.it

**DI TUTTI?**

# Zone e Domini

DI TUTTI?  
→ NON NECESSARIAMENTE



# Definizioni

- **Domain name per un host**
  - Sequenza di label che va dall'hostname (la foglia dell'albero di naming), costituita dalla label più a sinistra, al top dell'albero di naming mondiale, costituita dalla label più a destra
- **Dominio (riferito alla struttura gerarchica dei nomi)**
  - Sottoalbero dell'albero di naming mondiale: TLD, SLD, ...
- **Zona (riferito all'organizzazione dei name server)**  
**Dati relativi ai nomi di un Dominio, meno qualche**
  - sotto-dominio quando è amministrato da autorità di livello inferiore

*Zona e Dominio possono coincidere o meno*

# Gerarchia dei server

- **I name server non hanno i dati di tutti i nomi**
- **I name server devono conoscere quali altri server sono responsabili di altre zone**
  - Tutti i server devono conoscere i root name server
  - I root name server devono conoscere i server dei TLD
  - In generale, ciascun name server deve conoscere almeno il name server della zona immediatamente superiore (p.es., il name server della zona ing deve conoscere il name server della zona unimo) e viceversa
  - Tuttavia, ciascun amministratore di una zona, può inserire tra i propri dati anche altri name server



## ***Gerarchia dei server (cont.)***

**→ Ne consegue che la gerarchia di name server risulta differente e molto più irregolare rispetto alla gerarchia dei nomi di dominio**

### **NOTA**

- Un singolo livello della gerarchia può essere partizionato tra server multipli
- Un singolo server può servire più zone
- **Forte dipendenza dalle scelte degli amministratori di zona per la configurazione del relativo name server**

# *Server primari e secondari*

- **Gli amministratori di sistema inseriscono i dati relativi ad una Zona in un master file, che è l'unica sorgente di dati autoritativi per quella Zona**
- **Ci sono due tipi di name server che possono fornire dati autoritativi:**
  - Primary o master server, che leggono i dati su di una Zona direttamente dal master file
  - Secondary server, che scaricano i dati di una Zona dal rispettivo server primario

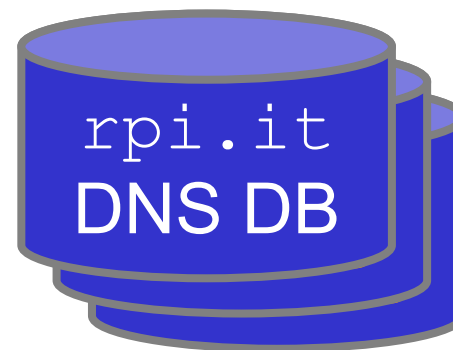
# Server primari e secondari (cont.)

- **Per ciascuna Zona, c'è sempre un server primario e vi può essere un certo numero di server secondari, che contengono una copia del database hostname-indirizzi IP**

Name server di `unimo.it`



Primario



Secondari

## *Server primari e secondari (cont.)*

- **I server secondari comunicano periodicamente con il server primario per verificare se i propri dati sono consistenti rispetto a quelli contenuti nel primario**
- **Se una copia di dati di un server secondario non è aggiornata, il server primario invia l'ultima versione**
- **La frequenza delle verifiche da parte del server secondario è stabilita dall'amministratore del sistema, ed il suo valore è tipicamente di uno/due volte al giorno**

# *Esempio*

- **Il ccTLD .it ha i suoi nameserver secondari distribuiti sia in Italia che nel mondo, in modo da garantire una raggiungibilità ed un livello di servizio ottimale**
- **Attuali nameserver secondari del ccTLD .it:**
  - m.dns.it – MIX S.r.L, Italia
  - r.dns.it – GARR, Italia
  - s.dns.it – Autonomica, Svezia
  - nameserver.cnr.it – CNR Pisa, Italia

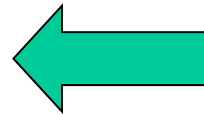
# *Attenzione a non confondere*

- **Name server primario (mantiene i dati della zona)**
- **Name server secondario (mantiene copie dei dati della zona)**
- **Authoritative name server (autoritativo relativamente ai dati di una zona)**

# *Classi di name server – i più visibili*

- **SLD name server**

- **Local name server**



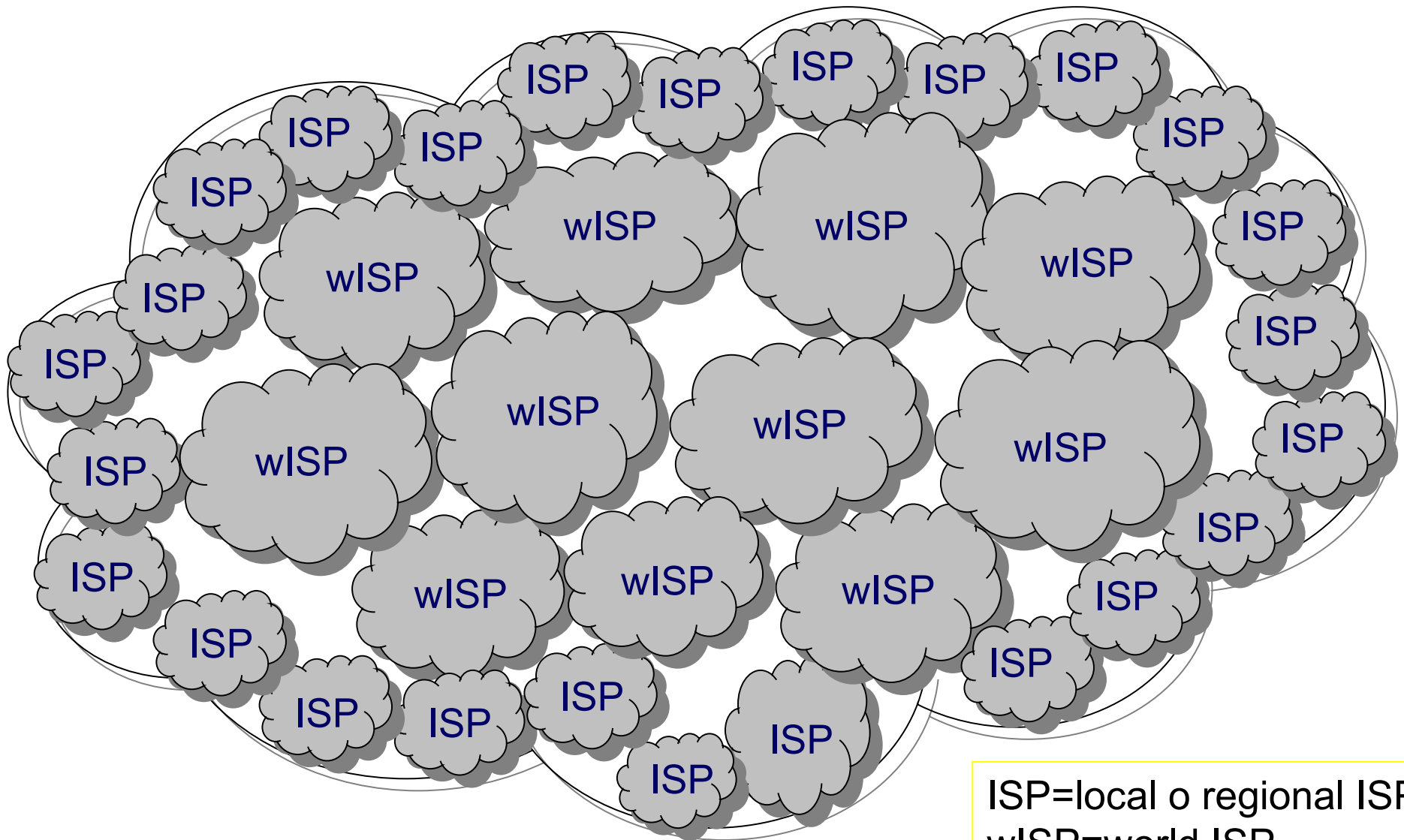
**(ogni ISP e organizzazione gestisce uno o più name server locali: sono le foglie dell'albero)**

# *Local name server*

- **Qual è?**
- **Quello che viene configurato (manualmente o automaticamente) dal client**
- **Possibilità:**
  - SO-HO senza dominio
  - Dominio con Contratto indiretto
  - Dominio con Contratto diretto
    - 1 zona (organizzazioni di medie dimensioni)
    - >1 zone (organizzazioni di grandi dimensioni, inclusa Università)

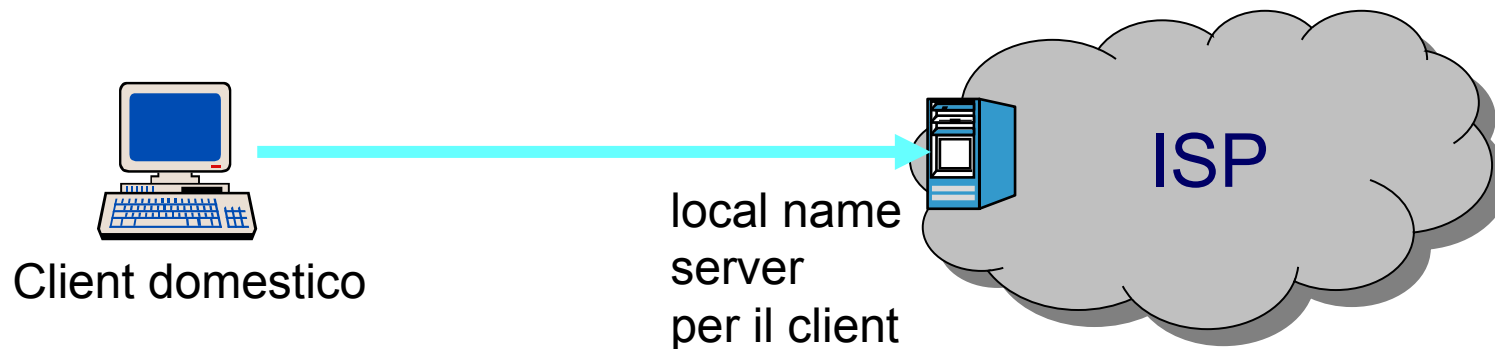


# Organizzazione di *INTERNET*



# ISP e DNS

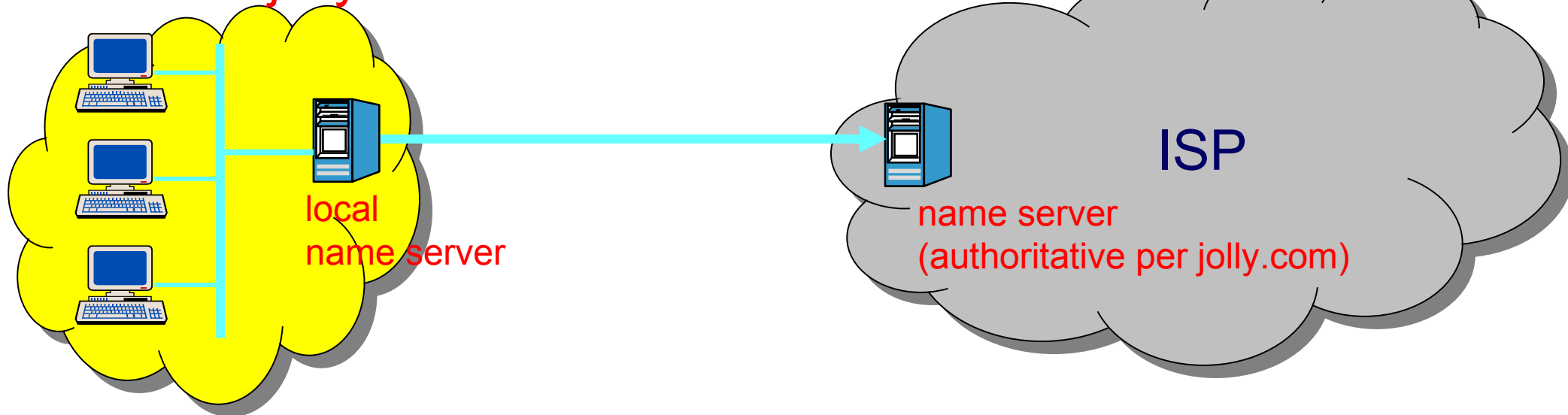
- **Ciascun ISP che gestisce un Point-of-Presence (POP), gestisce anche un server per la risoluzione dei nomi: name server**
- **Questo name server è il local name server per le utenze “domestiche” o SO-HO che non appartengono ad un dominio registrato**



# ISP e DNS

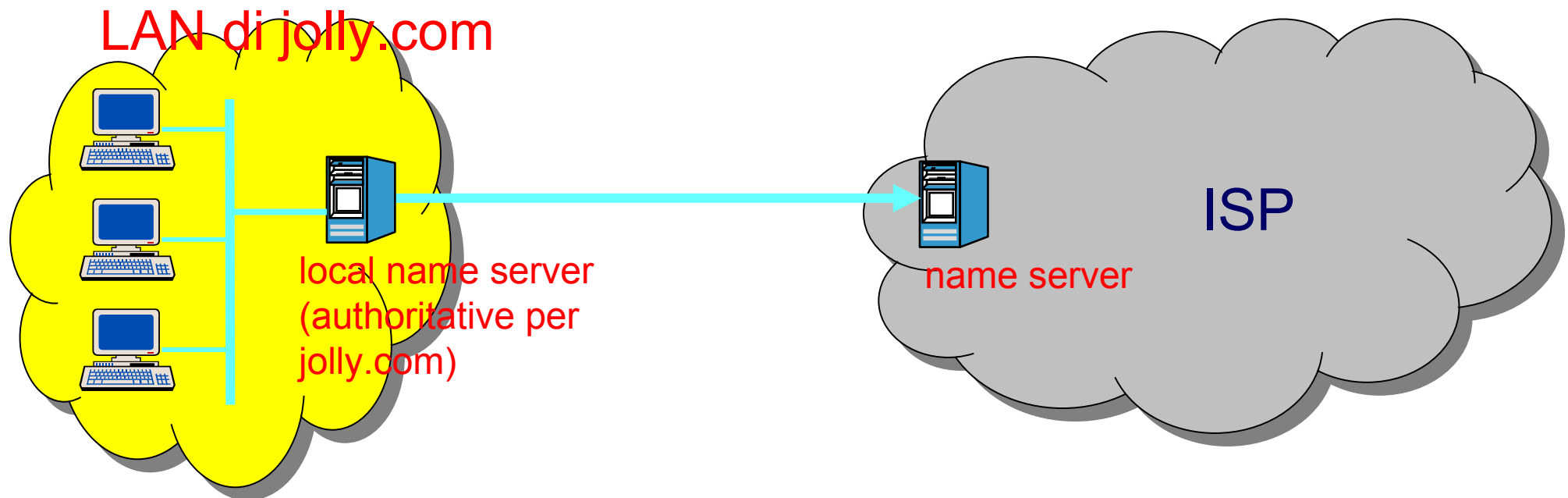
- **Client di organizzazioni con dominio registrato (es., jolly.com) con contratto indiretto (mediante un provider “delegato”, es., Aruba) funzionano in modo simile al precedente, con la sostanziale differenza che il name server dell’ISP è anche autoritativo per gli host del dominio jolly**
- **Jolly.com può o meno gestire un local name server**

LAN di jolly.com

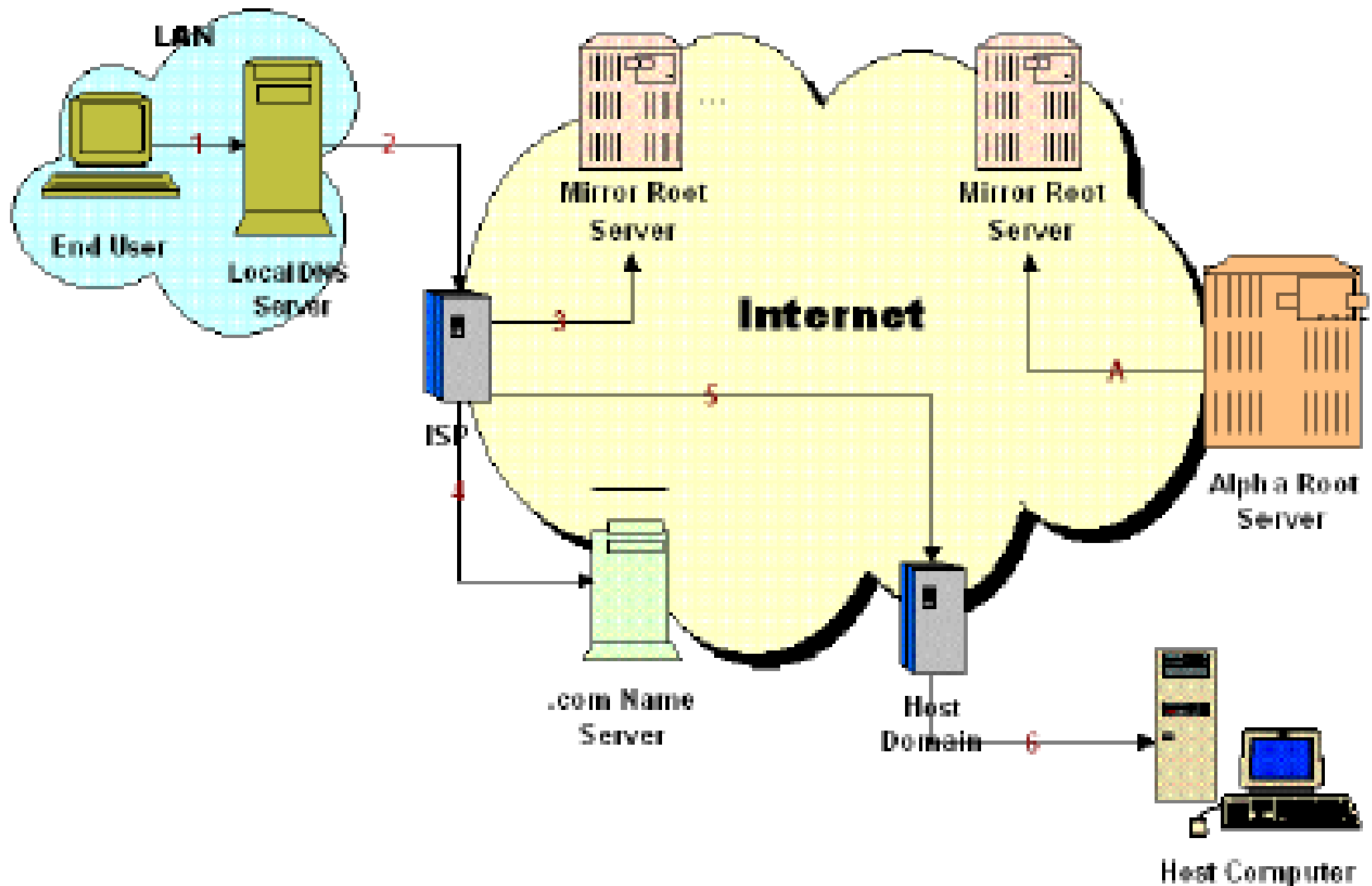


# ISP e DNS

- **Organizzazioni più grandi potrebbero gestire:**
  - un local name server con caratteristiche di authoritative se l'organizzazione ha in gestione (con “contratto diretto”) un dominio
  - molteplici name server locali e authoritative se vi sono più zone nel dominio jolly.com (come accade per l'università)



# Diversi livelli di name server



# *Gestione del caching dei dati*

- **Per ridurre i tempi di risposta, ogni name server del DNS è libero di effettuare il caching dei dati relativi ad altri server ed altre zone in modo da evitare di contattarli quando una risoluzione viene richiesta più volte**
- **I client che ricevono dati dalle cache dei name server sono informati che ciascun dato è fornito “as it is” e non è da considerare autoritativo**
- **A ciascun dato in una zona si assegna un valore time-to-live (TTL)**

# *Gestione del caching dei dati*

- **Quando un name server non-autoritativo ottiene un dato da un server autoritativo prende nota del TTL associato**
- **Il name server fornirà un dato nella cache al client che ne fa richiesta solo se il relativo TTL non è scaduto**
- **Se invece il TTL è scaduto, il name server contatta il name server autoritativo per controllare se il dato è valido o meno**

# Valore del TTL

- **Il caching è uno strumento potente per ridurre il traffico di Internet relativo alla risoluzione indirizzi**
- **La scelta del valore del TTL deve seguire tale scopo ed è a carico dell'amministratore della zona:**
  - Quando ci si aspetta che i dati di una zona cambino con poca frequenza, l'amministratore dovrà utilizzare TTL elevati
  - Al contrario, in zone soggette a frequenti cambiamenti, è opportuno che il TTL abbia valori bassi



# Componenti del DNS - INDICE

- **Zone e Name Servers**

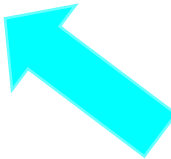
→ Ovvero i possessori e gestori dell'informazione, con le funzionalità di server abilitati a rispondere alle query dei client e di altri server

- **Domain Name Space e Resource Records**

→ Ovvero i dati su zone, descrittori, informazioni

- **Resolvers**

→ Ovvero i (primi) client del sistema DNS che sottomettono query per informazioni su hostname e indirizzi IP per conto delle applicazioni Internet



# ***Dati del database di una ZONA***

- **Dati relativi a tutti i nomi di un Dominio, meno alcuni sotto-domini amministrati da autorità di livello inferiore. Per esempio, una zona potrebbe contenere i dati di `ing.unimo.it`, meno quelli relativi a `weblab.ing.unimo.it`**
- **Hostname ed indirizzi IP del o dei name server che forniscono dati autoritativi per la Zona (si possono ritenere consistenti e ragionevolmente aggiornati)**

# ***Dati del database di una ZONA***

- **Hostname ed indirizzi IP dei name server che possiedono dati autoritativi per sottosezione delegate**
- **Parametri relativi alle modalità di gestione della Zona. Es.**
  - per gestire caching/replica delle informazioni
  - per gestire modalità e frequenza degli aggiornamenti

# ***Resource Records (RR)*** ***(Descrittori di risorsa)***

- **Legati ai nodi nell'albero del DNS**
  - Tutti i nodi terminali hanno RR
  - La maggior parte dei nodi non terminali hanno RR
  - Tutti i RR in una zona hanno la classe della zona
- **Ciascun RR contiene:**
  - Nome del dominio (simbolico)
  - Time-To-Live (TTL) del RR espresso in secondi
  - Classe del RR
  - Tipo del RR
  - Valore del RR (indirizzo IP numerico)

# Resource Records (RR) (Esempio)

- **Resource Record di:**

**www.unimo.it**

**134.56.26.68**

- Nome del dominio           www.unimo.it
- RR Time-To-Live (TTL)       86400 (in secondi)
- RR Class                    IN       (=INternet)
- RR Type                     A        (=Address)
- RR Value                    134.56.26.68

# *Tipi di Resource Records*

- **Oltre ai Resource Record di tipo A con informazioni hostname-to-IPaddress, i database del DNS contengono altre informazioni, ovvero Resource Records di altri tipi**

# Tipi di Resource Record (RR Type)

- **SOA**: Start Of Authority (parametri per gestire la zona)
- **NS**: Name Server autoritativo per una zona
- **A**: Host Address (indirizzo IP)
- **MX**: Mail eXchanger (dominio che accetta email, coppie <host, pref.>)
- **CNAME**: Canonical NAME per un alias: Un host può avere più hostname di cui uno canonico (canonical name) ed altri alias
- **PTR**: PoinTeR to another node (nome per indirizzo IP, per reverse lookup)
- **HINFO**: Host Information (descrizione CPU e Sistema Operativo)
- **TXT**: arbitrary TeXT (in formato ASCII)

# ***Esempio RR: Start of Authority (SOA)***

- **TTL – Time To Live - Determina per quanto tempo il record sarà valido sul server, senza richiedere un refresh**
- **Serial – identificatore seriale di aggiornamento; server per verificare che un server secondario abbia l'ultimo record con i dati più aggiornati**
- **Refresh – indica ad un server secondario quanto frequentemente deve richiedere un aggiornamento al server primario**
- **Expire – Tempo limite che indica per quanto tempo un file di ZONA può essere servito; utilizzato solo nel caso in cui il server primario non risponde per un lungo periodo di tempo**
- **Retry – Se il server secondario richiede un refresh ed il primario è irraggiungibile, il valore Retry indica quanto tempo attendere prima di provare nuovamente**



# *Esempio RR: Start of Authority (SOA)*

## **Esempio**

```
@ IN SOA mcs.vuw.ac.uk mark.comp.vuw.ac.uk (  
199610140 ; Serial number  
28800 ; Refresh 8 hours  
7200 ; Retry 2 hours  
604800 ; Expire 7 days  
86400 ) ; Minimum 24 hours
```

# ***Esempio RR: Name Server (NS)***

- **Specifica i server che contengono dati autoritativi relativi ad una Zona**
- **In particolare, indica il server primario e le informazioni sui server secondari che vengono utilizzati nel caso in cui il primario è irraggiungibile**
- **Quando si aggiungono nuovi server alla RootZone per il dominio, i relativi hostname e indirizzi devono essere aggiunti manualmente al file della LocalZone**

## **Esempio**

**@ IN NS      downstage.mcs.vuw.ac.uk**

## *Altri esempi di RR*

- **A -Address**

**Il tipo di record più comune. Usato per il riferimento da un nome (es., WWW) all'indirizzo IP di un host (es., 66.26.153.214). Le implementazioni più vecchie non consentivano che due record A contenessero lo stesso indirizzo IP. Questo vincolo è stato rimosso a causa della diminuzione di disponibilità di indirizzi IP.**

**embassy    IN    A    130.195.6.15**

**proto    IN    A    130.195.5.12**

## *Altri esempi di RR*

- **CNAME - Canonical Name**

**Tipicamente utilizzato per unificare i record e limitare le modifiche da effettuare quando un indirizzo IP cambia. Un CNAME agisce sia come record MX sia come record A. Un CNAME non può contenere un indirizzo IP. Deve essere un alias di un record A già esistente.**

**www IN CNAME proto**

## *Altri esempi di RR*

- **MX – Mail Exchanger**  
**L'unico record che consente di specificare una “priorità”. Specifica a quale server inviare una e-mail in arrivo. E' possibile specificare fino a 128 server, ciascuno con una priorità differente. La priorità più comune è pari a 10.**
- **AAAA – IPv6 Address**  
**Identico ad un tipico record A-Address, con l'unica differenza che gestisce I nuovi indirizzi IP del protocollo IP versione 6.**

# *Esempio di file DNS*

```
laser.net. IN NS ns1.granitecanyon.com.  
laser.net. IN NS ns2.granitecanyon.com.  
laser.net. IN NS ns1.secondary.com.  
laser.net. IN NS ns2.secondary.com.  
laser.net. IN TXT "LASER lmtl., NIC Handle: CIK72"  
laser.net. IN A 64.39.26.186  
laser.net. IN MX 10 mail.laser.net.  
www IN CNAME laser.net.  
mail IN A 63.116.218.133  
imap IN CNAME mail.laser.net.  
smtp IN CNAME mail.laser.net.  
webmail IN CNAME laser.net.  
localhost IN A 127.0.0.1  
ftp IN CNAME CIK.NO-IP.COM
```

Uso di NSLOOKUP

# Componenti del DNS - INDICE

- **Zone e Name Servers**

→ Ovvero i possessori e gestori dell'informazione, con le funzionalità di server abilitati a rispondere alle query dei client e di altri server

- **Domain Name Space e Resource Records**

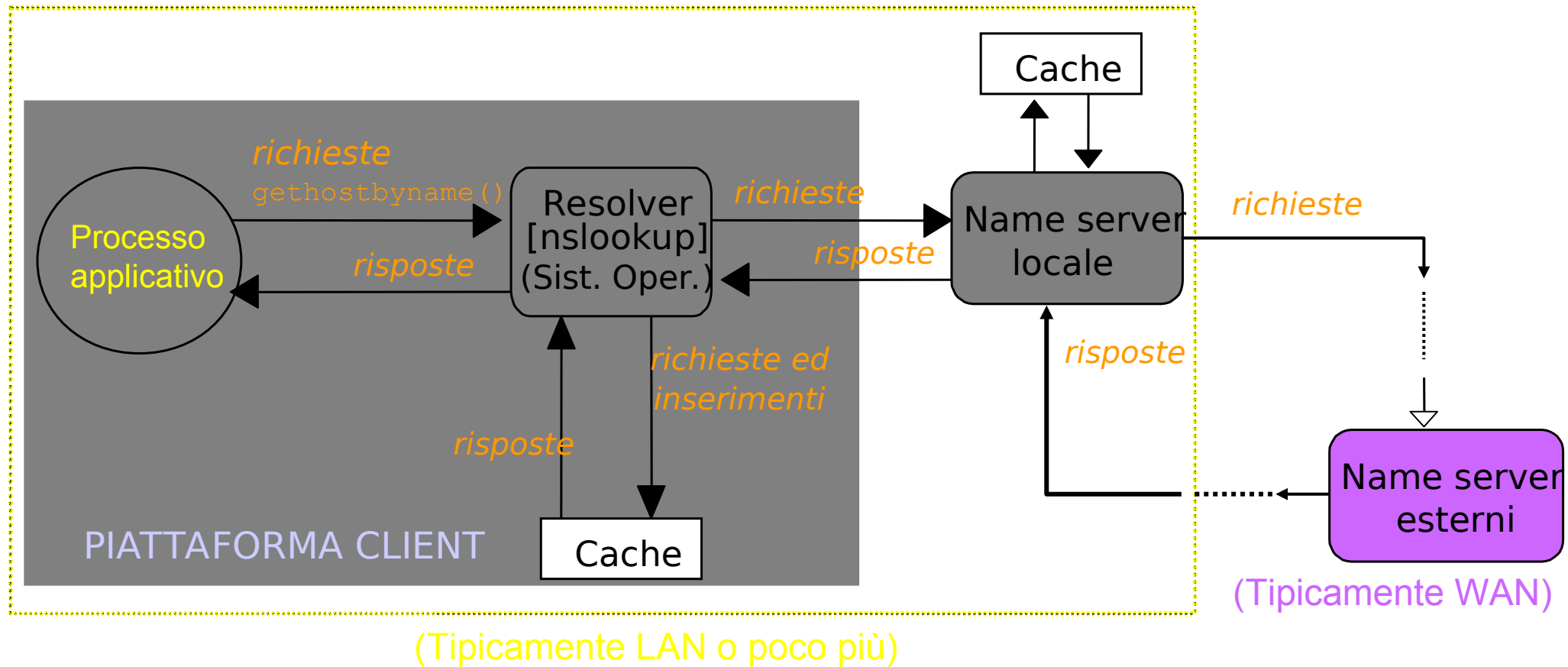
→ Ovvero i dati su zone, descrittori, informazioni

- **Resolvers**



→ Ovvero i (primi) client del sistema DNS che sottomettono query per informazioni su hostname e indirizzi IP per conto delle applicazioni Internet

# Resolver (lato client)



La maggior parte dei sistemi Linux/Unix hanno il file `/etc/resolv.conf` che contiene il dominio locale e gli indirizzi dei name server per quel dominio



# *Dati client*

- **Ogni resolver deve conoscere il riferimento ad almeno un name server locale**
- **La maggior parte dei sistemi Linux/Unix hanno il file `/etc/resolv.conf` che contiene informazione sulla Zona Locale e gli indirizzi del/i name server per quella Zona**
- **`/etc/resolv.conf`  
domain mit.edu  
128.113.1.5  
128.113.1.3**

# *Formato richiesta messaggio DNS*

**HEADER Section** (id., num. richieste, num. risposte,...)

**QUERY Section** (Domain Name, Type, Class)

*Response* **RESOURCE RECORDS**

*Response* **AUTHORITY RECORDS**

*Response* **ADDITIONAL INFORMATION**

# Flag del messaggio (16 bit)

- **QR** - Operation: *Query*=0, *Response*=1
- **QT** - Type: *Standard*=0, *Inverse*=1, *Obsolete*=2,3
- **AA** - Set if Authoritative Answer
- **TC** - Set if Truncated Response (> 512 bytes)
- **RD** - Set if Recursion Desired
- **RA** - Set if Recursion Available
- **Rcode** - Return code: *No\_error*=0, *Format\_err*=1, *Server failure*=2, *Nome non esistente* =3

# *Informazioni del RR di risposta*

- **Domain Name**
- **Response type**
- **Classe (IP)**
- **Time-To-Live (in secondi)**
- **Dimensione dei dati del RR di risposta**
- **Dati del Resource Record di risposta**

# Utilizzo di protocolli TCP e UDP

Quale protocollo di trasporto usa il DNS?

- **Nell'ambito del DNS, si utilizzano sia il protocollo UDP sia il protocollo TCP:**
  - Il protocollo TCP per il trasferimento di interi database da server primari a server secondari (replica)
  - Il protocollo UDP per il lookup (di singoli o pochi nomi)
  - Se nel lookup, la risposta necessita di più di 512 byte (nel caso di interi gruppi di nomi), il richiedente risottomette la richiesta utilizzando il protocollo TCP

# *Perché si può usare UDP nelle query?*

- **L'informazione da trasmettere è tipicamente piccola**
- **Molte informazioni sono distribuite tra più name server**
- **Considerando che il requisito velocità è indispensabile, viene preferito all'affidabilità**

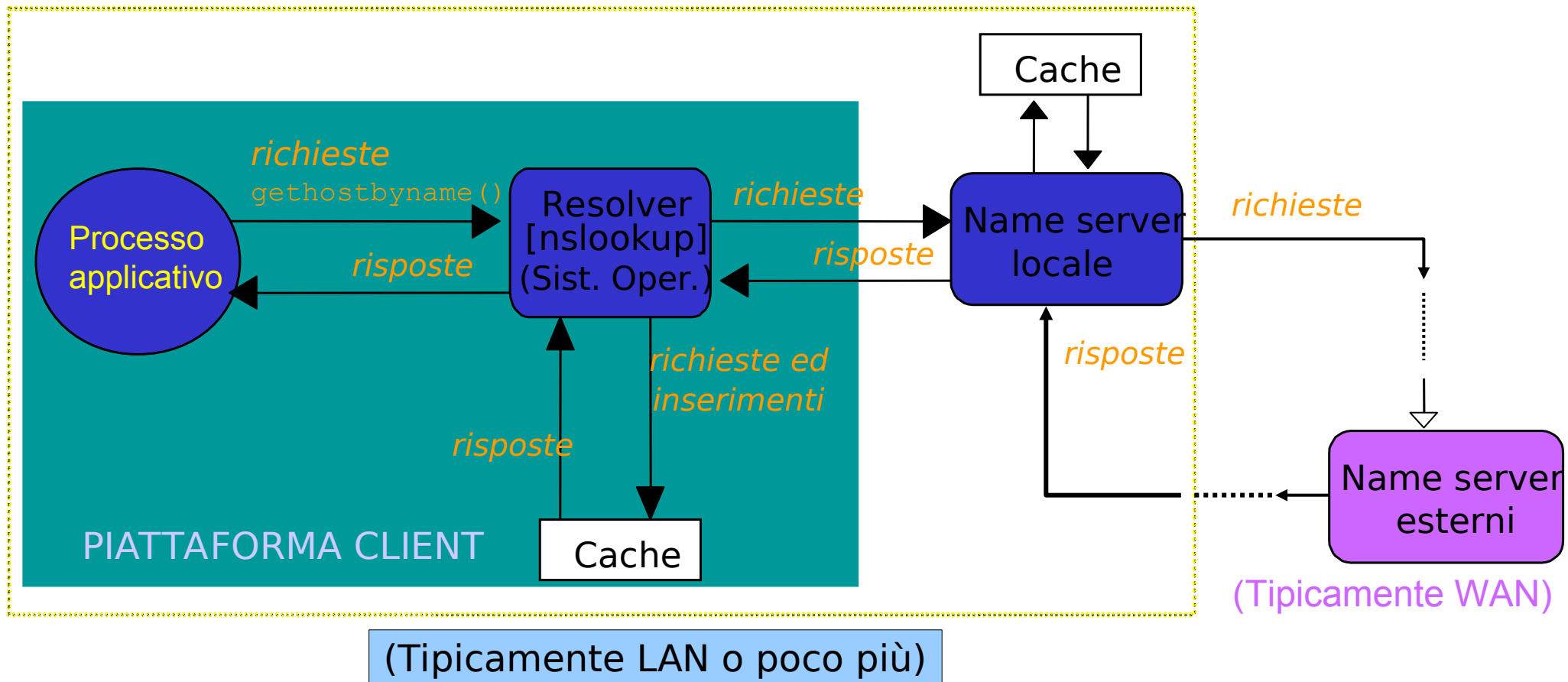
## **Modulo 4: Meccanismo distribuito di risoluzione dei nomi**

# *Sistema DNS: Meccanismo di risoluzione*

- **Nessun name server ha tutte le corrispondenze tra hostname e indirizzo IP**
- **Gli applicativi di rete utilizzano un meccanismo distribuito (client/server) per la risoluzione dei nomi (Lookup phase) attivato dalla componente Resolver del client**



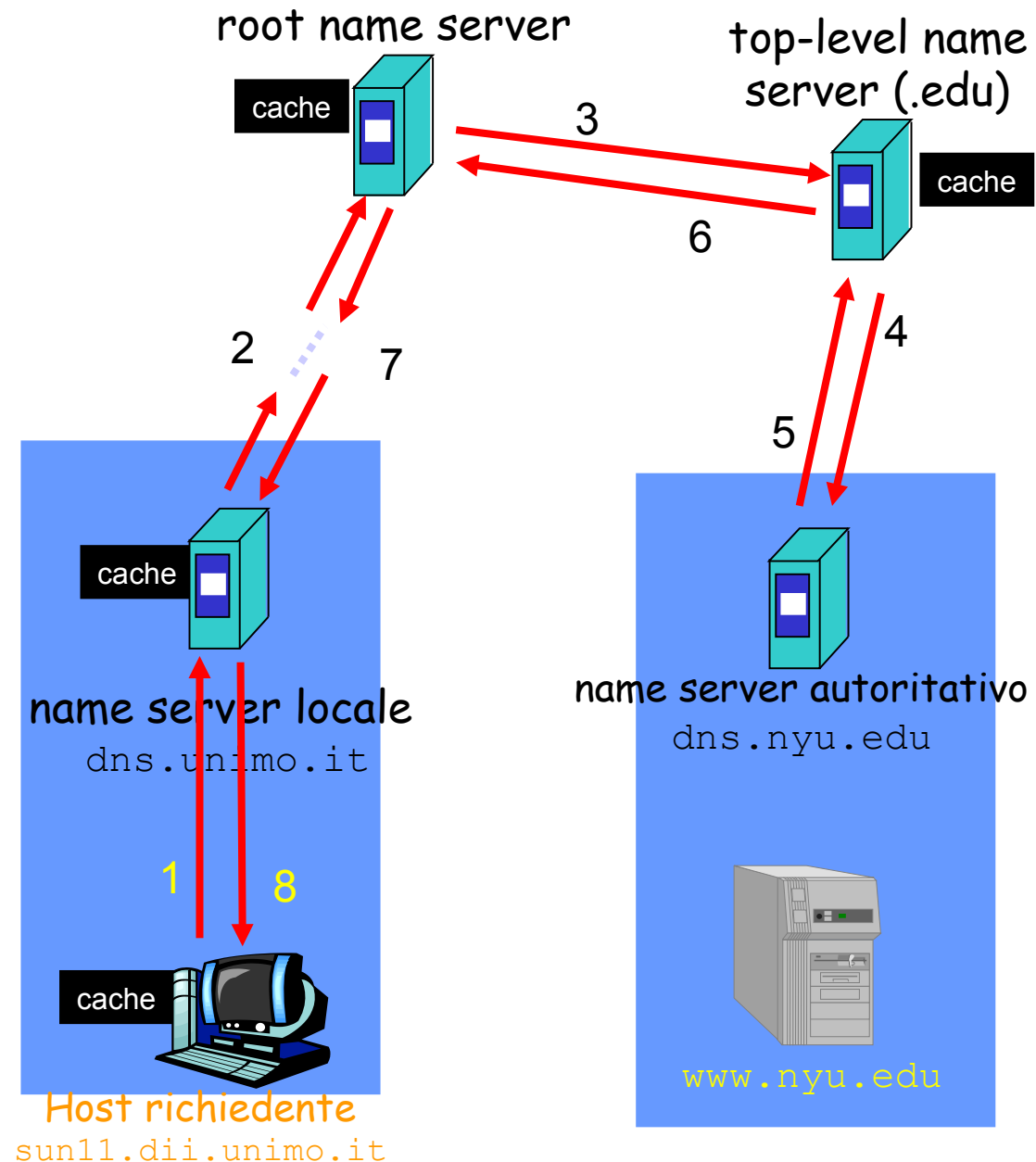
# Resolver (lato client)



# Sistema DNS: address resolution

L'host sun11.dii.unimo.it vuole conoscere l'indirizzo IP dell'host www.nyu.edu

- 1) Contatta il suo *DNS locale*
- 2) Se necessario, il *DNS locale* può contattare altri DNS intermedi, ed eventualmente uno dei *root DNS*
- 3) Se necessario, il *root DNS* contatta il *DNS autoritativo* per quell'indirizzo (o un *top-level DNS* nel caso in cui non conosca un *DNS autoritativo* per quell'indirizzo)



# Tipi di query

**Ciascun name server può effettuare due tipi di query nella risoluzione di un nome:**

- **Query ricorsiva**

- Il server, contattato e non in grado di risolvere il nome richiesto, assume un ruolo di client nei confronti di un altro name server.
- Più costosa in termini computazionali

- **Query iterativa**

- Il server, contattato e non in grado di risolvere il nome richiesto, risponde con i nomi di uno o più server da contattare

- **I root name server (e anche i TLD server) usano la configurazione iterativa.**

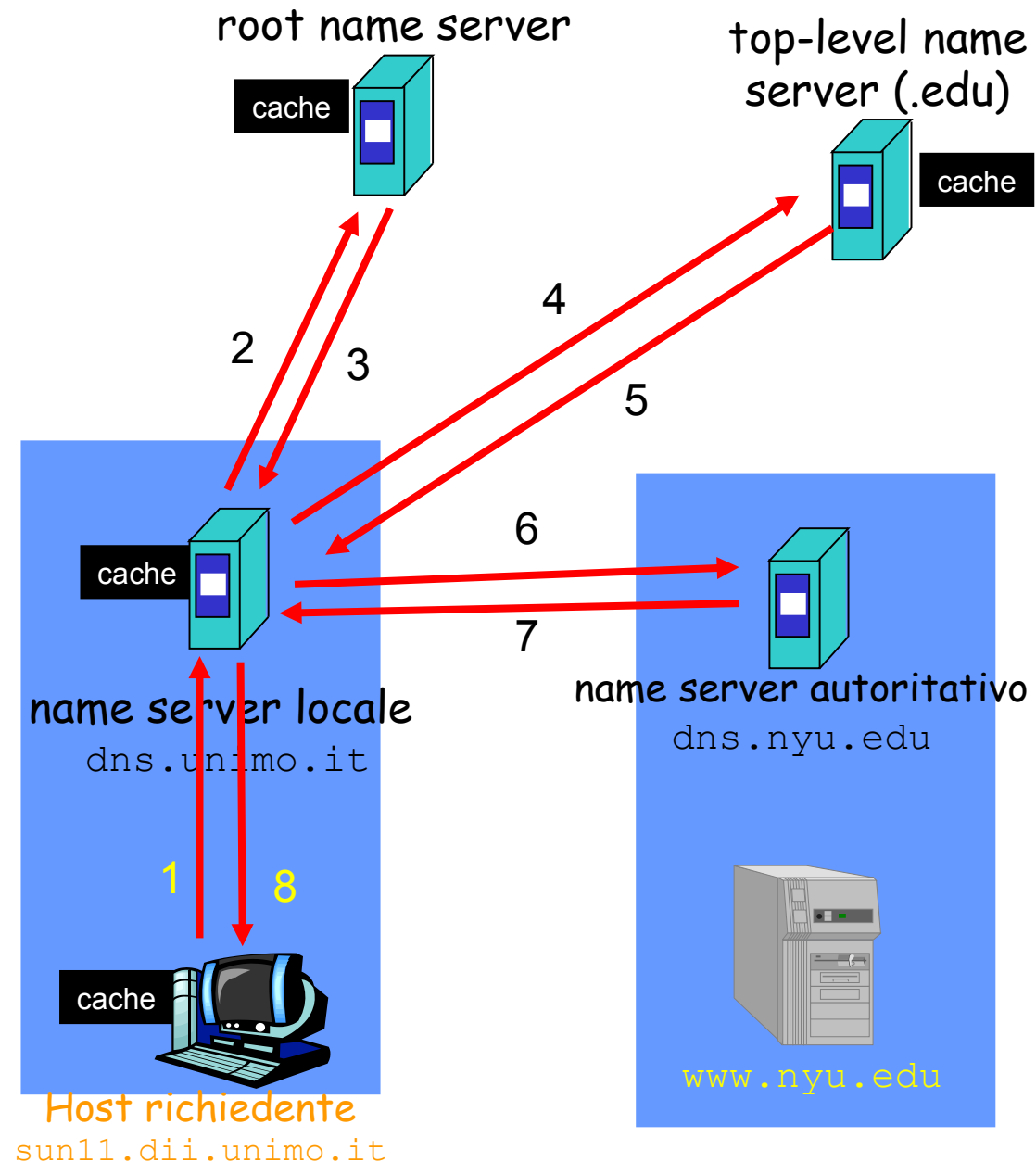
- Perché?

# Sistema DNS: address resolution (2)

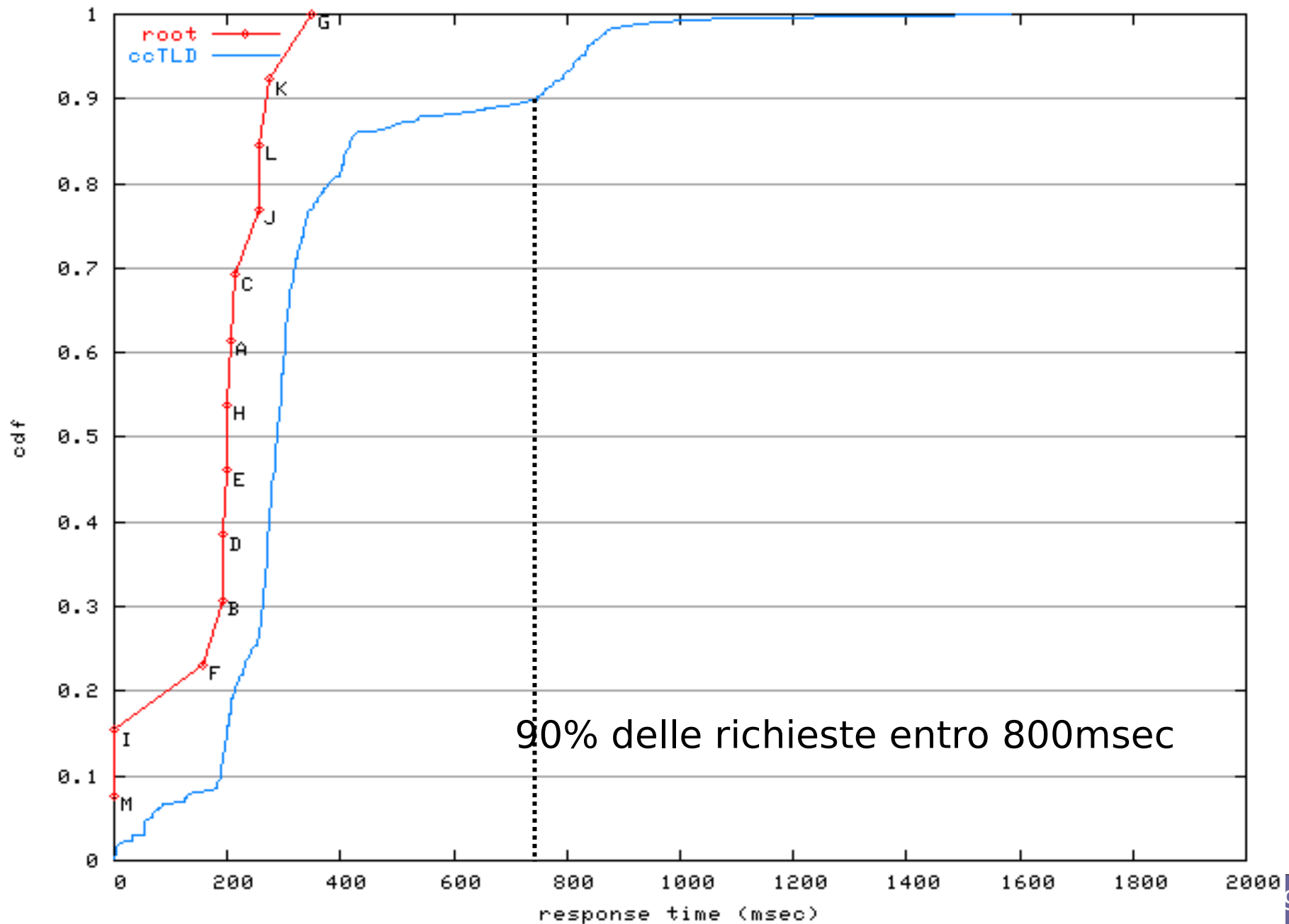
L'host `sun11.dii.unimo.it` vuole conoscere l'indirizzo IP dell'host `www.nyu.edu`

Poiché i root name server e i TLD name server ricevono molte richieste, per limitare il sovraccarico, utilizzano la risoluzione iterativa

Gli altri name server, ad esclusione degli authoritative, tipicamente utilizzano la risoluzione ricorsiva

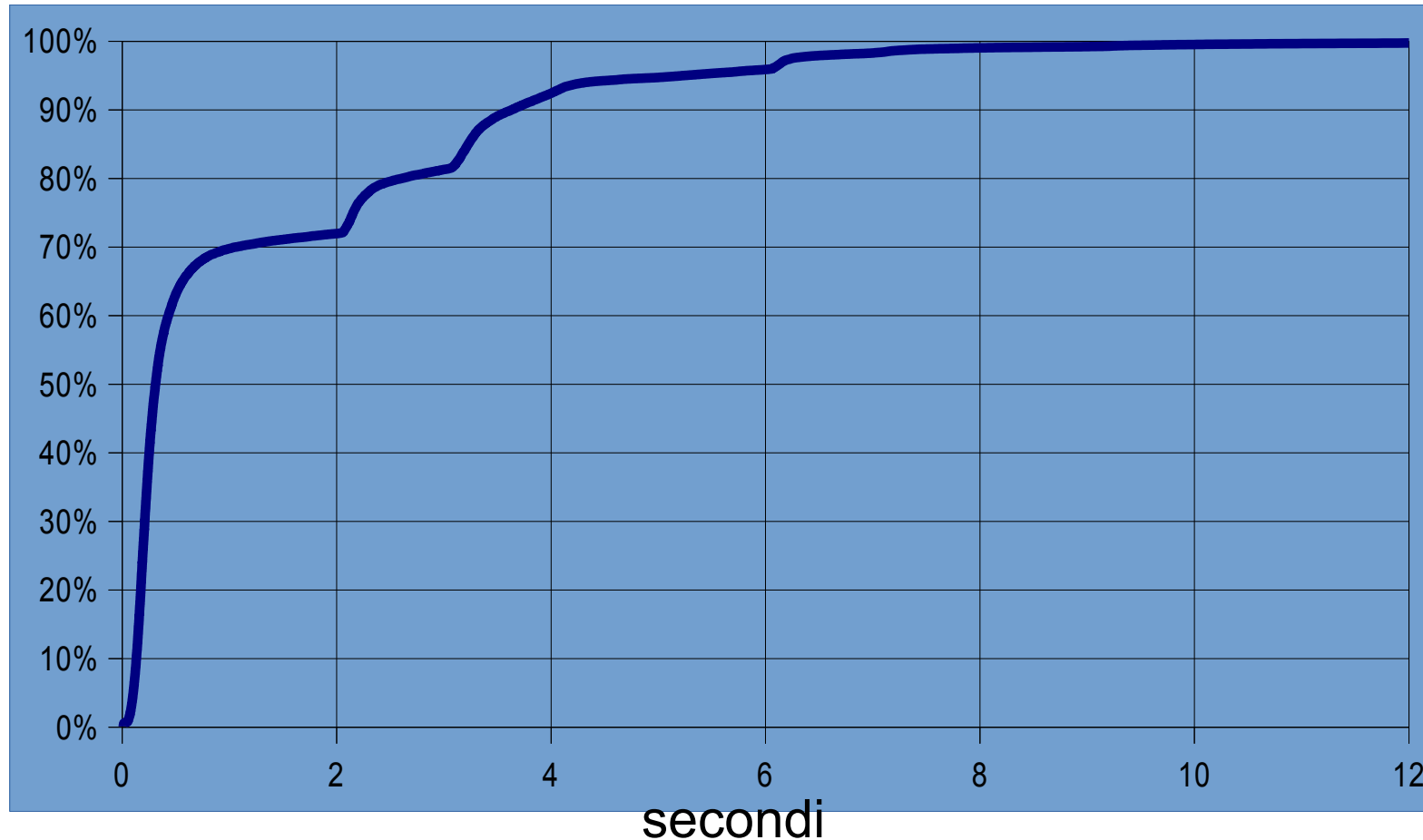


# Tempi per la risoluzione root e TLD



# Tempi per la risoluzione mediante DNS

(2002 - domini random: 70% entro 2s, 90% entro 4s)



I nomi di domini popolari hanno tempi inferiori (perché?)