DOMAIN NAME SYSTEM (DNS)

DNS

Un'applicazione Internet al servizio delle applicazioni Internet

1. Introduce un altro livello di *naming* in Internet, oltre gli indirizzi IP, che risulta "più vicino all'utente", ma non solo per questo motivo
2. E' un esempio di sistema distribuito geograficamente che funziona molto bene
3. Poco noto, ma fondamentale per acquisire informazioni (ambito ***forensics***) e come sistema da proteggere molto bene (ambito ***cyberdefense***)

INDICE

1. Identificatori degli host
2. Organizzazione logica dello spazio dei nomi
3. Name server
4. Authoritative name server e *Zone*
5. Dati del DNS: *Resource Record*
6. Meccanismo distribuito di risoluzione dei nomi
7. Registrazione e organizzazione

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*) possono avere due (o più) identificatori:
  - **Indirizzo IP** (***numero di 32 bit***): utilizzato per indirizzare e instradare i pacchetti nella rete
  - **Hostname** (***stringa alfanumerica di al più 255 caratteri***): nome logico utilizzato tipicamente dalle persone

… gli *hostname [1]*

- **Sequenza di *label* separate da punti**
- **Ogni label si compone di al più 63 caratteri**
  - **Consentiti caratteri alfanumerici e alcuni simboli secondo certe regole**
  - **Possono essere interpretati da software secondo regole di internazionalizzazione (Internationalized Domain Name – IDN) per la visualizzazione di altri simboli**
- **L'intero hostname può essere di al più 255 caratteri**

… gli *hostname [2]*

- **Sequenza di *label* separate da punti**

Esempi

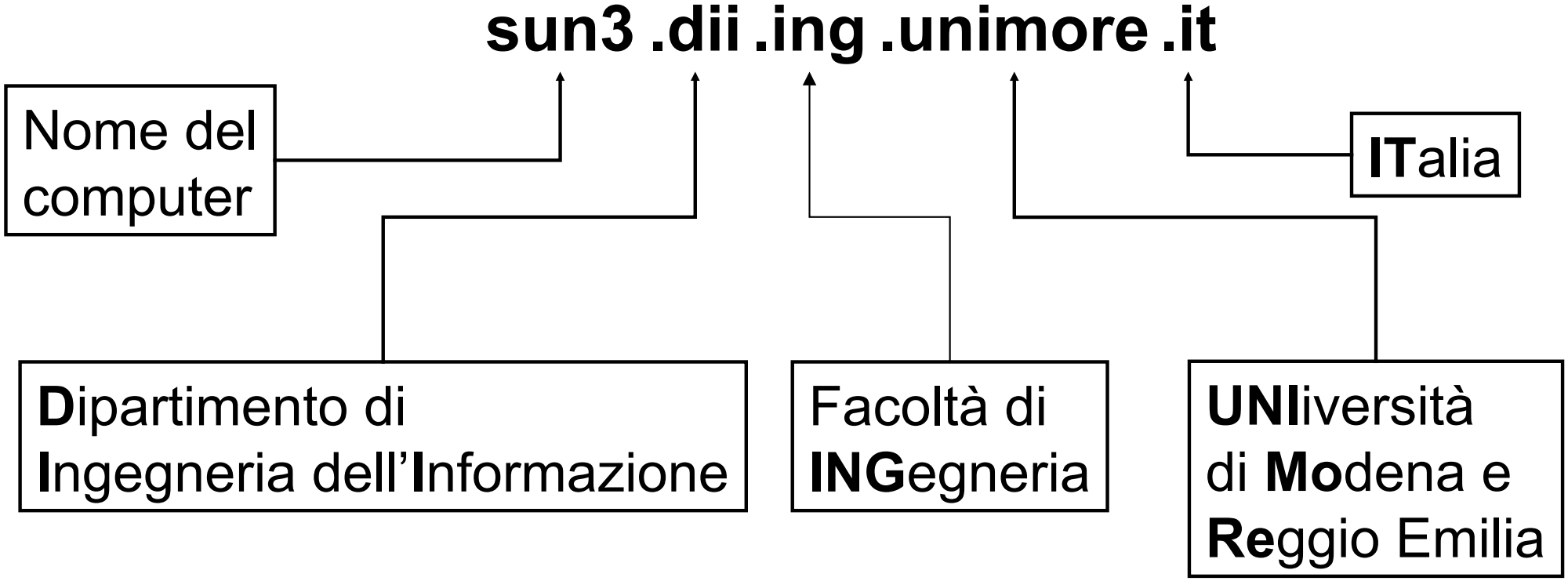
- w3c.org
- samba.ing.unimo.it
- www.unimo.it
- promo.dim.ing.unimo.it

Non c'è alcuna corrispondenza tra le label dell'hostname e 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?

Altra motivazione oltre l'usabilità

- Specificare l'indirizzo di un host con un valore pre-fissato renderebbe l'interazione client/server più veloce (eviterebbe la fase di lookup), ma:
  - il software del client dovrebbe essere ricompilato ogni volta che il software del server venisse spostato su di un altro host
  - il server non potrebbe usare più di un host per erogare il servizio
- *In contesti avanzati, un singolo hostname potrà corrispondere a più indirizzi IP*

Altra motivazione oltre l'usabilità

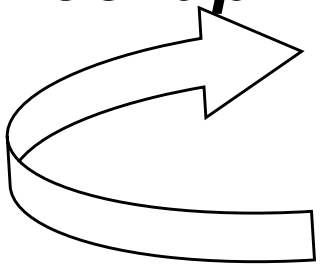
- L'uso dell'**hostname** è un buon compromesso che, effettuando il collegamento (***binding***) tra hostname e indirizzo IP a tempo di esecuzione dell'applicazione e non al tempo di implementazione medesima, consente e facilita:
  - la rilocabilità dell'applicazione server su altro server
  - l'uso di uno o più server per ospitare un'applicazione
  - l'uso di alias per un hostname

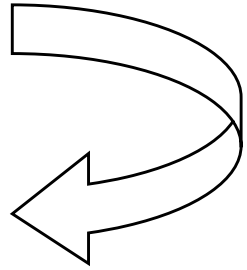
Compromesso: si preferisce *maggiore flessibilità* a scapito di una minima perdita di efficienza in fase di lookup

2 meccanismi di *naming* → necessità di traduzione

Reverse Lookup

Hostname: **sun3.dii.ing.unimore.it**





Indirizzo IP: **134.56.26.68**

(10000110.00111000.00011010.01000100) ***Lookup***

Traduzione da hostname e 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) - 1

1. Realizza uno spazio dei nomi gerarchico e permette la traduzione del nome mnemonico di un host in un indirizzo IP e viceversa

Domain Name System (DNS) - 2

2. Implementa un meccanismo efficiente per "risolvere" un hostname in un indirizzo IP e viceversa utilizzando:
   - **molteplici *name server* distribuiti in tutta Internet**
   - **deleghe gerarchiche di competenze a multipli server**
   - **uso di caching a tutti i livelli**
   - **uso di protocollo di trasporto "veloce" (UDP) per le query DNS (lookup)**
     - **Oggi ci può anche essere supporto a TLS e HTTPS**
   - **uso di protocollo di trasporto "affidabile" (TCP) per gli aggiornamenti dei record dei name server**

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

Importanza del DNS

- **Commerciale**: valore economico dei nomi
- **Funzionale**: se il sistema DNS non funziona, non funzionano molti servizi basati su Internet, e la stragrande maggioranza degli utenti non riuscirà ad accedere ai servizi
- **Tecniche informatiche**
- **Sicurezza**: *pharming*, *cache poisoning*, *DNS amplification*

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**
  - yahoo**.com**
  - amazon**.com**
  - facebook**.com**
  - …

Regole sintattiche di *naming*

- I nomi possono contenere solo i seguenti caratteri: "a-z", "0-9", e il simbolo "-" (trattino)
- I nomi non devono iniziare e finire con il simbolo "-"
- Non è ammesso registrare domini che nei primi quattro caratteri contengono la stringa "xn--“
- La lunghezza del nome ammessa può variare da un minimo di 3 ad un massimo di 63 caratteri
- Si possono usare indifferentemente caratteri minuscoli e maiuscoli

Norme fondamentali di *naming*

- Nomi a dominio assegnati dalla RA in ordine cronologico di richiesta
- Nomi a dominio riservati (comuni, regioni, università, …)
- Nomi a dominio NON prenotabili
- La procedura di assegnazione è conclusa quando avviene il caricamento nel database dei nomi a dominio

Principio di delega del DNS

- Una volta che un'organizzazione ha registrato il SLD presso il registrar del TLD, l'amministratore del SLD:
  - **ha controllo completo sugli altri campi del nome a dominio**
    - Il significato dei segmenti (sotto-domini) è delegata all'organizzazione
    - Non vi è limite sul numero di sotto-domini o numero di livelli
    - Lo spazio dei nomi non è correlato ad una interconnessione fisica. Per esempio, mat.unimo.it e dii.unimo.it potrebbero trovarsi sullo stesso piano di un edificio o in città differenti
  - **deve garantire la risoluzione di tutti i nomi esistenti nell'ambito del dominio registrato inclusi tutti gli eventuali sottodomini**

Il valore del Second-Level Domain

- I nomi SLD hanno un valore economico perché sono associati con i beni/servizi prodotti e con la reputazione dell'organizzazione
- Esempio:
  - Gran parte del valore della società Amazon era dato dal suo nome di dominio Amazon.com
  - Dati 2003:
    - Valore azionario: 10 miliardi$
    - Valore beni: 2 miliardi$

Consequenze del valore dei nomi

- Il commercio dei nomi può avere costi molto elevati
- Registrazione di nomi facili da ricordare e che conducono ad una categoria di prodotti/servizi. Es., car.com, house.com, garden.com

- Chi ha diritto alla registrazione di un nome?
  - Il sig. Ferrari può registrare il dominio ferrari.it?
  - L'azienda di spumanti Ferrari può registrare il dominio ferrari.it?

Cybersquatting

- ***Cybersquatting***: registrare un dominio che assomiglia o contiene il brand di un'azienda e provare a rivenderlo

- Il cybersquatting ha portato all'adozione di regole come l'***Anticybersquatting Consumer Protection Act*** (**ACPA**) e un sistema di politiche di arbitrato da parte dell'ICANN

Regole per dispute

- ***Anticybersquatting Consumer Protection Act* (ACPA)**
- Sistema di politiche di arbitrato incluse le ***Uniform Dispute Resolution Policy*** (UDRP) dell'ICANN

  http://www.icann.org/udrp/
- Risoluzione delle dispute nel **ccTLD .it**

  http://www.nic.it/documenti/regolamenti-e-linee-guida/risoluzione-delle-dispute-nel-cctld.it-regolamento-versione-2.0.pdf

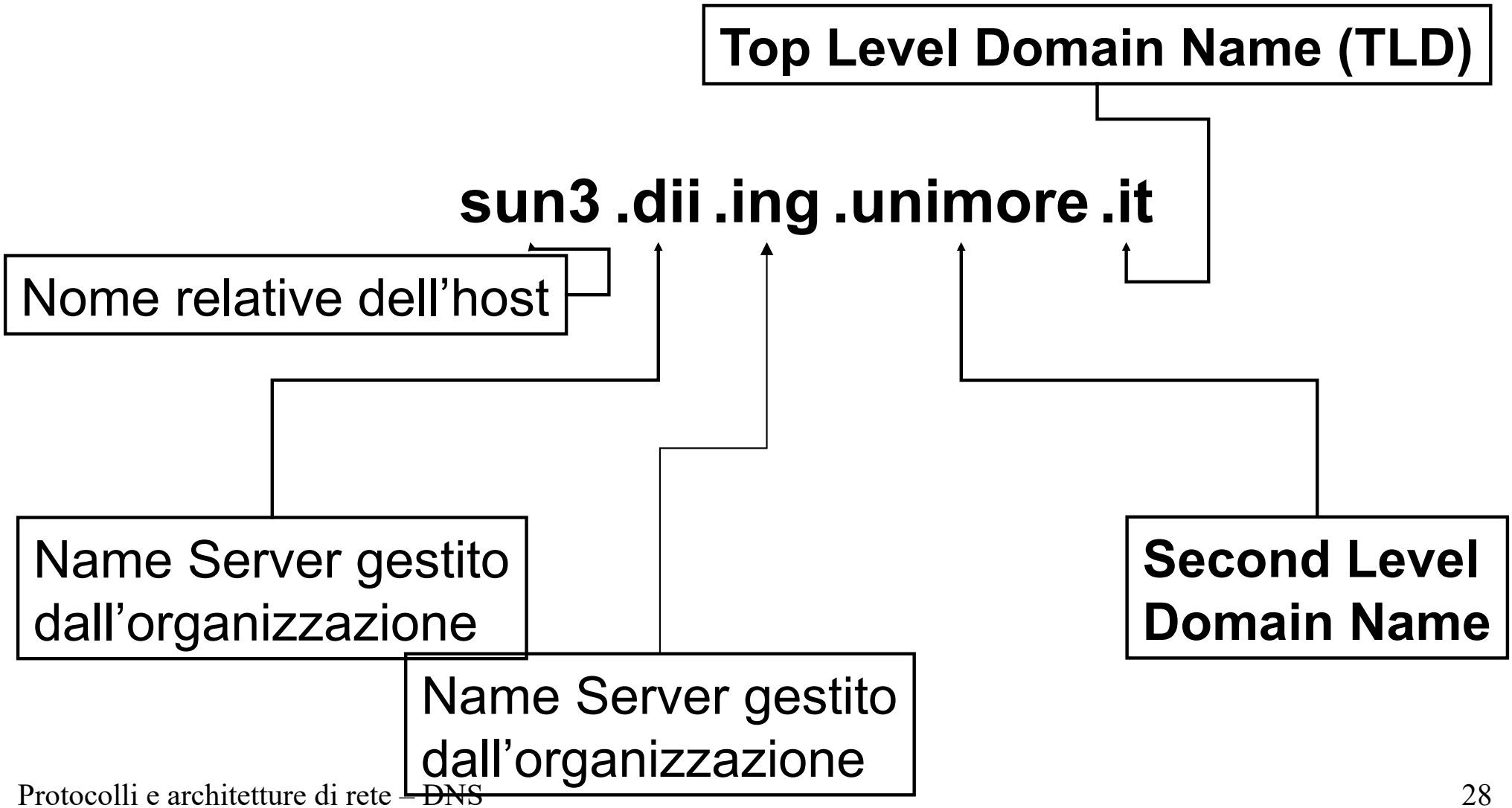
Punycode

- Attualmente è possibile registrare nomi di dominio con simboli **unicode**
- Il termine punycode identifica dei simboli differenti che assomigliano o sono indistinguibili l'uno dall'altro all'occhio umano
  - Possono essere teoricamente utilizzati per attaccare protocolli sicuri (ottenere un certificato digitale per un dominio di cui si ha il controllo «indistinguibile» da uno noto – vedremo meglio con cenni di protocolli sicuri)
  - Per questo, non tutti i simboli unicode sono accettati per formulare nomi di dominio

2. Organizzazione logica dello spazio dei nomi

Hostname (*canonico*)

- **Le diverse parti di un hostname**



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**

Top Level Domain (TLD) "storici"

Nome del Dominio	*Significato*
COM	Organizzazioni commerciali (*free registration*)
EDU	Istituzioni USA per l'istruzione
GOV	Istituzioni governative USA
MIL	Istituzioni militari USA
NET	Maggiori centri di supporto per la rete (*free registration*)
ORG	Organizzazioni senza scopo di lucro (*free registration*)
ARPA	Dominio della rete ARPANET (*amministrazione*)
INT	Organizzazioni internazionali
Codice nazionale (it, ch, fr, jp, uk, ...)	240 nomi nazionali (*schema geografico*): **ccTLD** [Caso interessante: Tuvalu con dominio **.tv**]

‘Nuovi’ TLD

- 2002: Sponsored and Unsponsored TLDs
  - **Unsponsored TLD (uTLD) – TLD of a community that follows ICANN regulations**
    - **.biz (www.NIC.biz)**
    - **.info (www.NIC.info)**
    - **.name (www.NIC.name)**
    - **.pro**
    - **.eu (*europe*)**
  - **Sponsored TLD (sTLD) – TLD of a community that follows its own regulations**
    - **.museum**
    - **.coop**
    - **.aero**

Dal 2012: liberalizzazione

- L'ICANN amplia il numero dei gTLD esistenti ben oltre i 19 finora accettati
- Dal 2013 è possible utilizzare qualsiasi tipo di parola e in qualsiasi lingua, incluse quelle non latine: cirillico, arabo, cinese
- Costo (stimato): circa 185.000$ per ogni dominio più 25.000$ ogni anno di rinnovo

Elenco TLD attivi

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

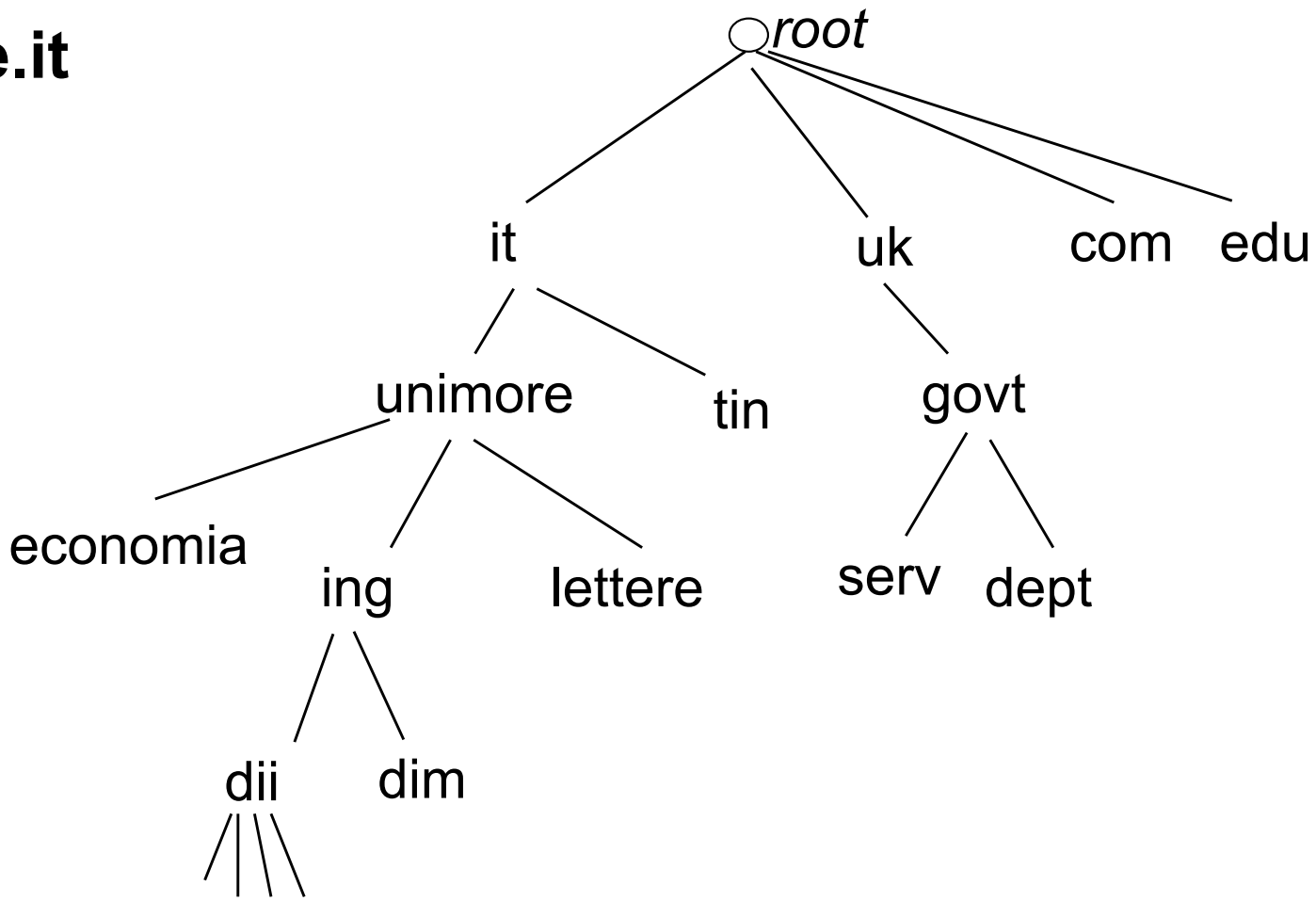
Second-Level Domain (SLD)

- **Tipicamente corrispondono ai veri *brand* di una 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 un professore dell'Università di Modena e Reggio Emilia, penso a **<nome.cognome>@unimore.it**
- I nomi hanno anche un valore economico

Organizzazione gerarchica dei domini

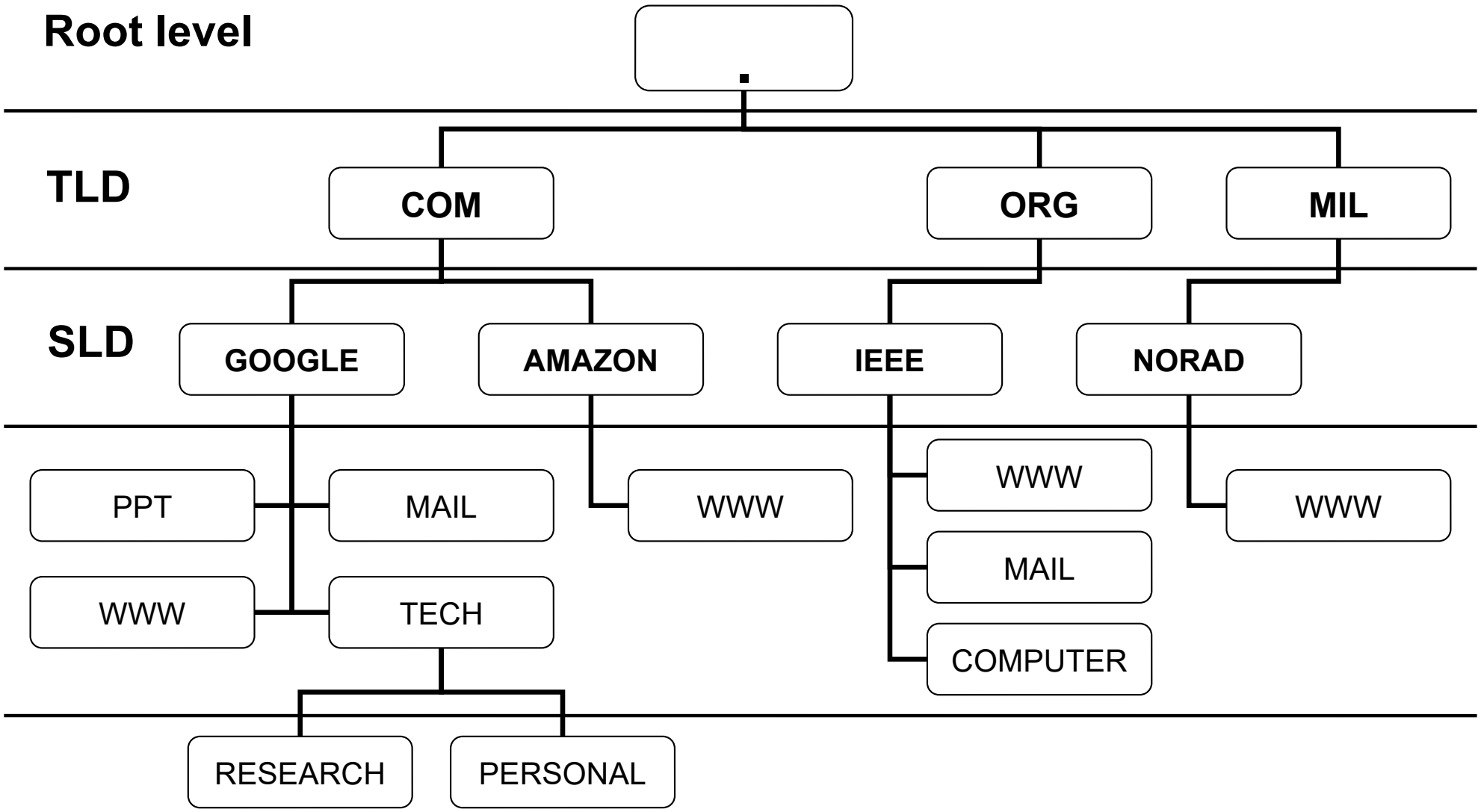
- **dii.ing.unimore.it**
- **dept.govt.uk**

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



Esempio: Università di Modena “unimore”, 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 dei domini



3. Name server

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)**

Piattaforme dei root name server (*cont.*)

- I root 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 a Internet (dal livello 1 al livello 3)
- **I root name server B-M sono costituiti da più macchine (oltre 130 in più di 50 Paesi diversi), anche se ciascun name server è "logicamente uno"**

http://www.root-servers.org/

- **"Internet continuerà a funzionare, anche se 2/3 dei root name server dovessero risultare irraggiungibili"** (RFC-2870)

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)

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

4. Authoritative name server (e Zone)

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

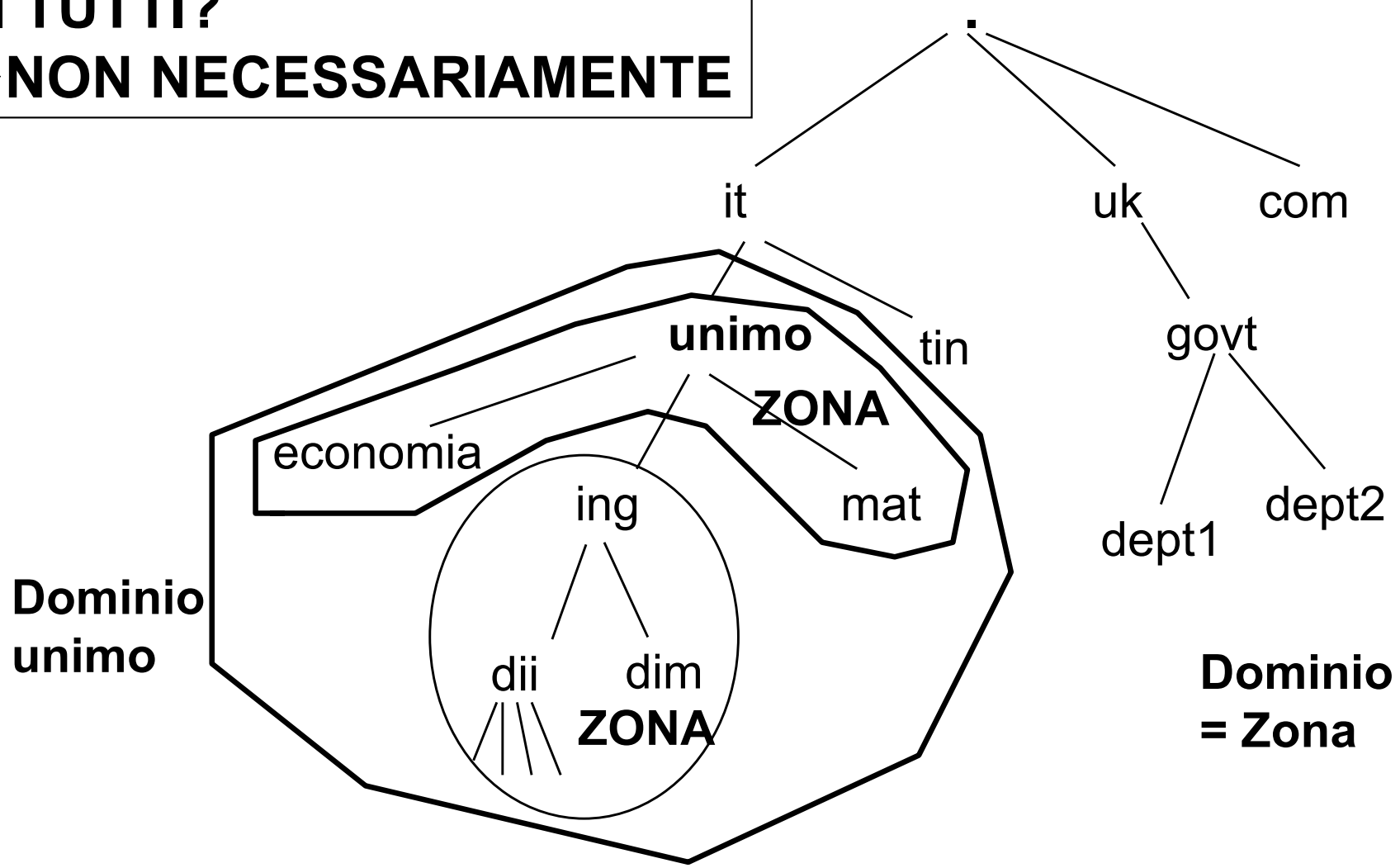
Esempio

- Qualche name server gestito dall'organizzazione **`UNIMORE`** è responsabile degli hostname in **`unimore.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**

5. Dati del DNS: *Resource Record*

Dati del DNS

- I name server sono de facto dei database distribuiti che contengono record su:
  - Zone
  - Indirizzi
  - Gestione server
  - Modalità di risoluzione indirizzi
  - …

Resource record

- Ci sono decine di tipi di resource record, anche se solo pochi sono usati comunemente.
- La maggior parte sono sperimentali, obsoleti o utilizzabili per scopi che raramente si presentano in pratica

Tipi di Resource Record (RR Type)

- **A**: **Record di Host Address e indirizzo IP** (il RR più noto) include l'associazione fra **canonical hostname** e indirizzo IP di un host
- **NS**: Record che descrive il **Name Server autoritativo** per una determinata zona
- **SOA**: **Start Of Authority**. Record che descrive i parametri relativi alla gestione la zona così come sono stati configurati dall'amministratore della zona
- **MX**: **Mail eXchanger**. Record relativo a un server che gestisce email per un determinato dominio.
  - In grandi sistemi, un dominio può avere multipli record MX fino a 128 (con priorità specificata a partire dal primary MX)
  - Un mail exchanger per un dominio non deve necessariamente far parte di quel dominio

Tipi di Resource Record (RR Type)

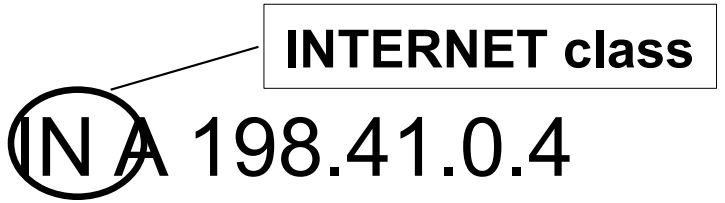
- **CNAME**: Canonical NAME per un alias: Un host può avere più hostname di cui uno canonico (*canonical name*) e altri definiti alias. Tipicamente utilizzato per unificare i record e limitare le modifiche da effettuare quando un indirizzo IP cambia. Un CNAME agisce sia come record MX sia come record A. Un CNAME non può contenere un indirizzo IP. Deve essere un alias di un record A già esistente
- **PTR**: PoinTeR to another node (per reverse lookup)
- **HINFO**: Host Information (descrizione CPU e Sistema operativo)
- **TXT**: in origine, arbitrary TeXT (in formato ASCII), ora impiegato per includere informazioni utili a diversi tipi di protocollo (esempio: SPF, si vedano email sicure)
- **AAAA – IPv6 Address**: identico a un record A, con l'unica differenza che gestisce i nuovi indirizzi IPv6

RR *Address* (A)

- 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)**
  - **Valore del RR (indirizzo IP numerico)**
  - **Time-To-Live (TTL) del RR espresso in secondi**
  - **Classe del RR**
  - **Tipo del RR**

RR-A esempio root



A.ROOT-SERVERS.NET. IN A 198.41.0.4

B.ROOT-SERVERS.NET. IN A 192.228.79.201

C.ROOT-SERVERS.NET. IN A 192.33.4.12

...

M.ROOT-SERVERS.NET. IN A 202.12.27.33

RR-A esempio

- **Resource Record** di:

  www.unimore.it ⟷ 134.56.26.68

  - **Nome del dominio**
  - **RR Time-To-Live (TTL)**
  - **RR Class**
  - **RR Type**
  - **RR Value**

www.unimore.it
86400 (in secondi)
IN (=**IN**ternet)
A (=**A**ddress)
134.56.26.68

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

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

```
@ 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
```

Dati del database di una ZONA

1. Dati relativi a tutti i nomi di un Dominio, meno alcuni sotto-domini amministrati da autorità di livello inferiore.
2. Hostname e indirizzi IP del o dei name server che forniscono ***dati autoritativi*** per la **Zona** (si possono ritenere consistenti e ragionevolmente aggiornati)
3. Hostname ed indirizzi IP dei name server che possiedono dati autoritativi per **sotto-zone** delegate
4. Parametri relativi alle modalità di gestione della Zona. Es.
   - per gestire caching/replica delle informazioni
   - per gestire modalità e frequenza degli aggiornamenti

Validità del contenuto del *name server autoritativo* per una zona

https://www.intodns.com

Provarlo con alcuni domini:

- unimore.it
- governo.it
- difesa.it
- repubblica.it
- facebook.it

6. 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

- Il DNS è un sistema client-server
- I resolver sono i (primi) **client** del sistema DNS che sottomettono query al loro *local name server* per risolvere indirizzi su hostname e indirizzi IP per conto delle applicazioni Internet
- Il resolver è di solito una piccola libreria compilata in ogni programma che richiede i servizi DNS

Dati client

- Ogni resolver deve conoscere il riferimento ad almeno un name server locale
- Su Windows è parte della configurazione delle Connessioni di rete nel pannello di controllo
- 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
```

Local name server

- Sono dei name server specializzati per intermediare le interazioni fra resolver e name server autoritativi per le diverse zone
  - Sono configurati per gestire ricorsivamente le richieste di risoluzione dei resolver
  - Svolgono ruolo di caching
- Possono essere gestiti in autonomia, o essere gestiti da altri (e.g., ISP, name server pubblici)
  - Vedere prossimo elemento degli argomenti (“Registrazione e organizzazione”)
  - Se configurati all’interno di un’organizzazione, possono risolvere direttamente i domini relativi alla zona dell’organizzazione (name server autoritativo che svolge ruolo anche di local name server)

“local” name server pubblici

Poiché la definizione del *local name server* è configurabile da parte di ciascun utente (con competenze per farlo), è anche possibile far riferimento a name server pubblici, quali:

- **Italia**
  - dns.nic.it: 193.205.245.5
  - dns2.nic.it: 193.205.245.8
- **OpenDNS - http://www.opendns.com/**
- **Google Public DNS**
  - IP 8.8.8.8 e 8.8.4.4
- **CloudFlare DNS**
  - IP 1.1.1.1

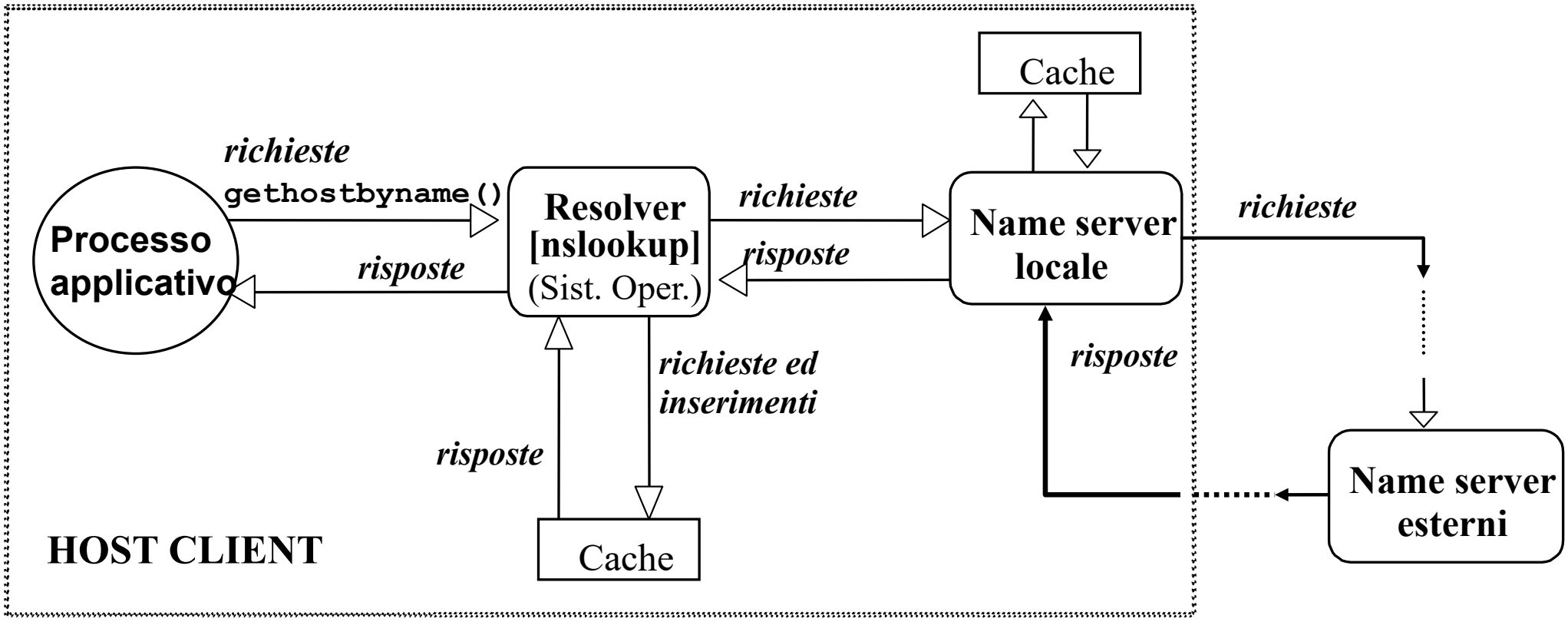
Tipi di query

Ciascun name server può essere configurato per rispondere a 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.
- **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 gli authoritative) sono configurati per rispondere a query iterative***
- ***I local name server tipicamente per query ricorsive (magari da client trusted)***

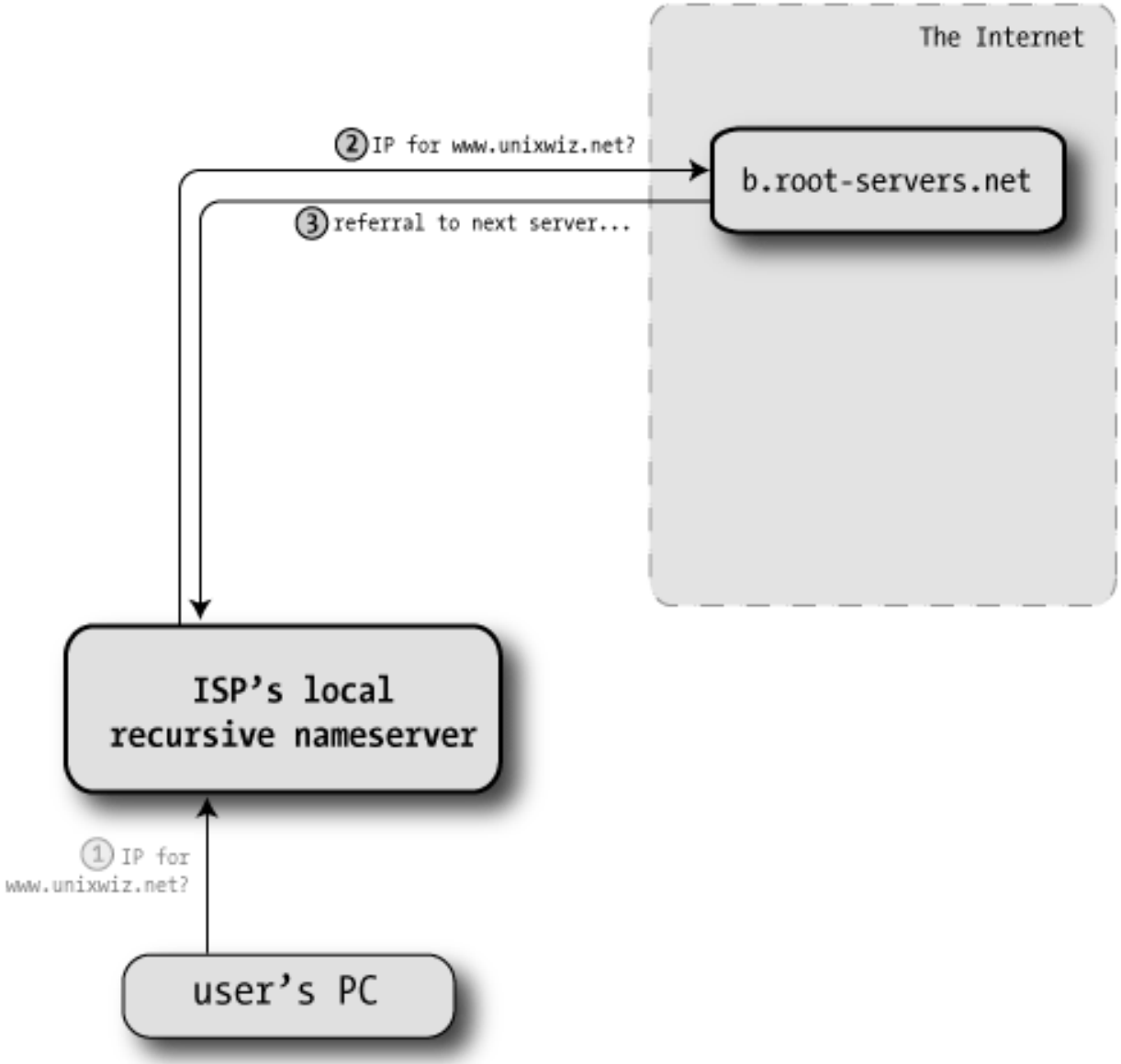
Perché?

Dns lookup (*lato client*)



Esempio: www.unixwiz.net

Il name server locale, configurato ricorsivamente, una volta che riceve la richiesta dal resolver [1] contatta un root name server (a caso nella lista o in sequenza) – nell'esempio b.root-servers.net – e gli invia [2] la query per il record di tipo A relativo a www.unixwiz.net



Fase [3] - richiesta

- Il root server non ha il RR di **unixwiz.net**, ma conosce il server del Global Top Level Domain (GTLD) che è responsabile del dominio **.net** domain
- La risposta è in forma di record **NS** contenente i server più qualificati a rispondere alla query dell'utente
- L'approccio è del tipo: "Go ask these servers - here's a list"

Fase [3] - risposta

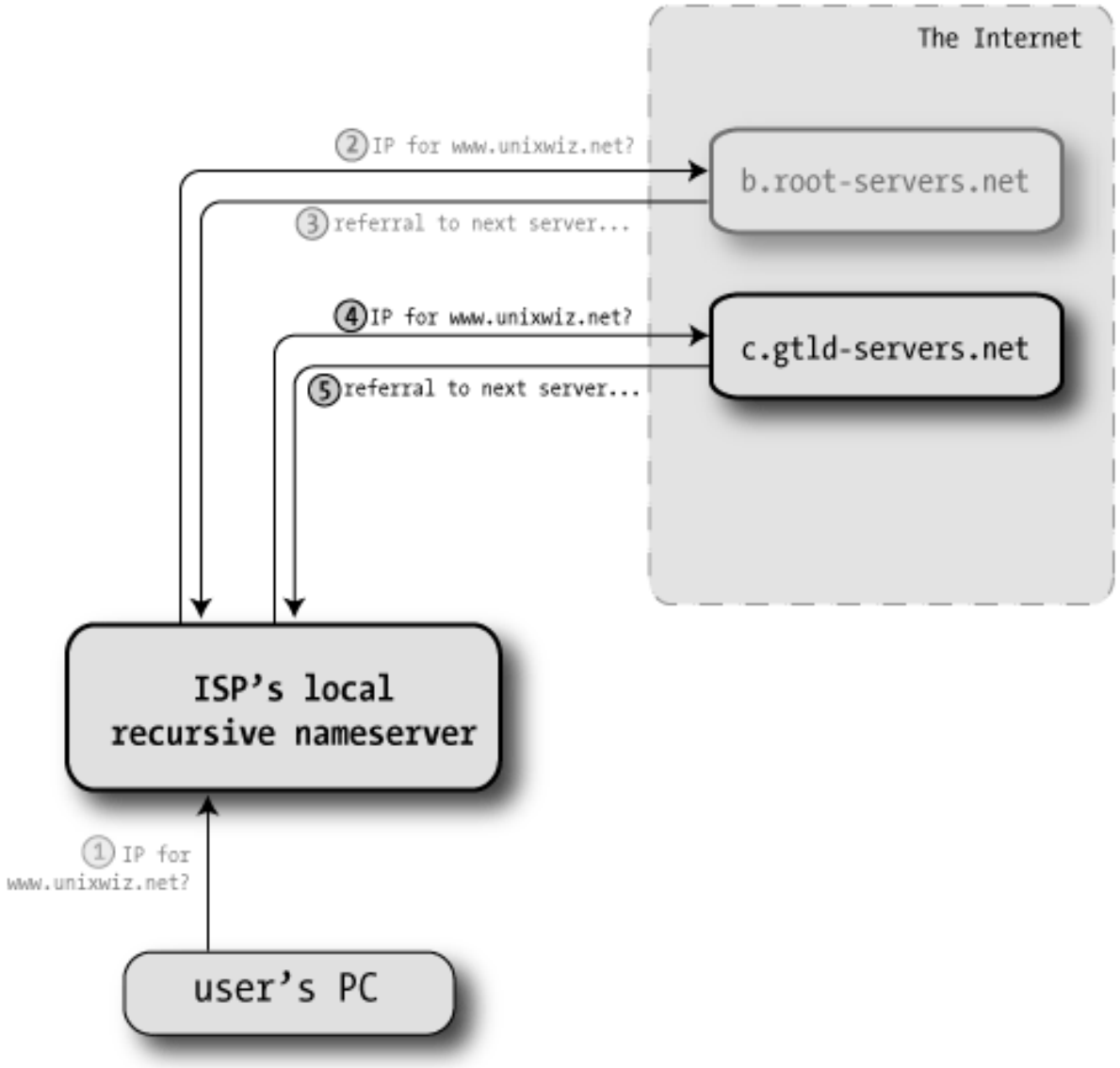
/* **Authority section** */
NET.
IN NS A.GTLD-SERVERS.NET.
IN NS B.GTLD-SERVERS.NET.
IN NS C.GTLD-SERVERS.NET.
...
IN NS M.GTLD-SERVERS.NET.

Anche se abbiamo chiesto solo i record NS, i root server ci forniscono anche i loro indirizzi IP: questa parte, detta “glue” (colla), serve per risparmiare tempo evitandoci un altro lookup

/* **Additional section - "glue" records** */
A.GTLD-SERVERS.net. IN A 192.5.6.30
B.GTLD-SERVERS.net. IN A 192.33.14.30
C.GTLD-SERVERS.net. IN A 192.26.92.30
...
M.GTLD-SERVERS.net. IN A 192.55.83.30

Fase [4] -richiesta

Il name server locale sceglie uno dei server autoritativi (nell'esempio **c.gtld-servers.net**) e gli invia la stessa query: "Qual è il record A per **www.unixwiz.net**?"



Fase [5] -risposta

- Il server GTLD non conosce la specifica risposta alla query ma conosce l'insieme di server che devono dare la risposta perché autoritativi sul dominio **unixwiz.net**

/* **Authority section** */

unixwiz.net.

IN NS cs.unixwiz.net.

IN NS linux.unixwiz.net.

/* **Additional section** - "glue" records */

cs.unixwiz.net. IN A 8.7.25.94

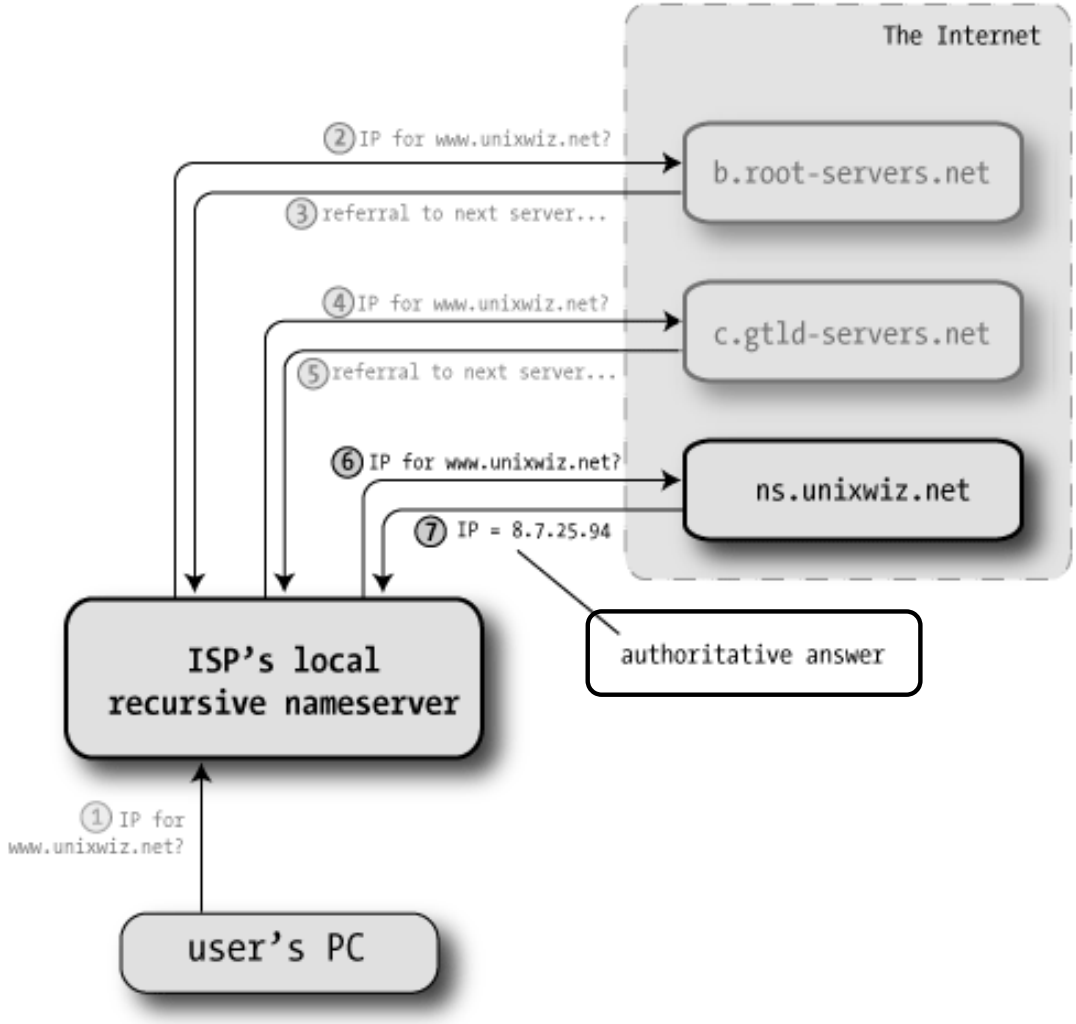
linux.unixwiz.net. IN A 64.170.162.98

Fase [6/7] – richiesta/risposta

Ancora una volta, il name server locale sceglie uno dei server autoritativi (in esempio **ns.unixwiz.net**) e gli invia la stessa query: “Qual è il record A per **www.unixwiz.net**?"

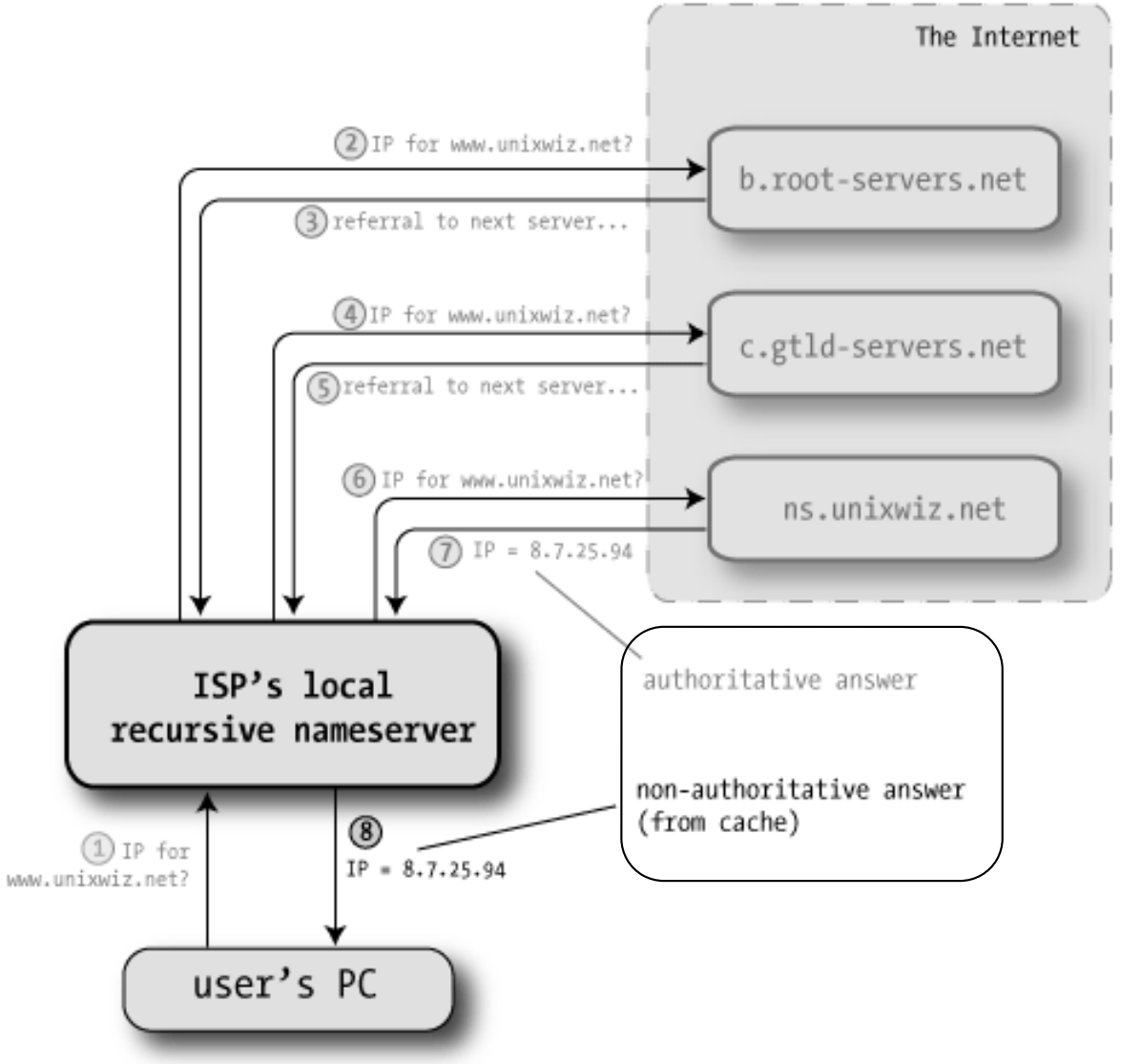
Questo server ha la informazione e fornisce il **record** A per **www.unixwiz.net**.

specificando "*This is an authoritative response*"



Fase [8] – risposta al client

Il name server locale memorizza il record A nella sua cache (nel caso in cui qualche altro client effettui la stessa query in seguito) e lo invia anche al client. La risposta al client non include l'indicatore *autorevole*. Anche se ha ricevuto la risposta da un server autoritativo, il name server locale non può dire al client che è la fonte dell'autorità informativa



PRESTAZIONI: 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) espresso in secondi**

Gestione del caching dei dati (*cont.*)

- 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, si dovranno utilizzare TTL elevati
  - In zone soggette a frequenti cambiamenti, è opportuno che il TTL abbia valori bassi
  - Per domini dove si vogliono ridirezionare le richieste tra molteplici host (google, amazon, akamai, …), è necessario che il TTL abbia valori molto bassi
  - Il valore di default del TTL è 86400sec (=1 giorno)

dig

- dig è un tool è eseguire query DNS
- Uso tipico:

  Lookup: `dig [<record-type>] <hostname/domain> [@nameserver]`

  Reverse: `lookup: dig –x <ip-address> [@nameserver]`
- Usi interessanti:
  - Componendo l'hostname in modo appropriato possiamo realizzare un *reverse lookup* tramite un *lookup* a record PTR
  - Con l'opzione `+norecurse` possiamo **disabilitare** il flag per richiedere **risoluzione ricorsiva** delle query inviate
  - Con l'opzione `+trace` possiamo usarlo per effettuare query iterative presso tutti i livello della gerarchia DNS, senza delegare il nostro *local nameserver*

Privacy delle query DNS

- Il protocollo di query DNS storico utilizza UDP
  - Ovvero, chiunque gestisce la nostra rete può conoscere gli hostname da noi ricercati
- Negli ultimi anni esistono alcune estensioni per garantire la **confidenzialità delle query dal *resolver* al *local nameserver*** tramite *incapsulamento in protocolli sicuri*
  - **DoT**: DNS over TLS
  - **DoQ**: DNS over QUIC
  - **DoH**: DNS over HTTPS (più supportato da browser)

Estensioni di sicurezza del sistema DNS: DNSSEC

- DNS può soffrire di un problema di ***autenticità*** dei record che otteniamo dalle nostre query
  - Motivazioni: uso intensivo di intermediari, ad esempio:
    - ***local nameserver*** che effettua query ricorsive «al posto nostro»
    - Uso intensivo di ***caching*** (vedere **DNS Cache Poisoning**)
- **DNSSEC** è un'estensione di DNS che prevede l'impiego di **firme digitali** per garantire l'autenticità dei record ricevuto
  - Materiale aggiuntivo necessario viene distribuito attraverso DNS stesso, ad esempio:
    - **DS**: Delegation Signer
    - **RRSIG**: Resource Record Signature
    - **NSEC3**: Authenticated *Denial of existence*

7. Registrazione o organizzazione

Ruoli e competenze in dettaglio

- ***Domain Name Authority***: L'entità che gestisce i servizi di root (oggi **ICANN**)
- ***Registration Authority***: Una entità che fornisce servizi di registrazione per un **TLD**
- ***Registrar***: Società intermedia autorizzata (dalla Domain Name Authority o dalla Registration Authority) che fornisce servizi di registrazione
- ***Registrant***: Sono i clienti dei servizi di registrazione che registrano un nome di dominio presso una Registration Authority o, più comunemente, presso un Registrar
- ***Maintainer***: Sono i gestori di un nome di dominio e devono garantire determinate competenze

Contact information del Registrant

- Contatti dell'amministrazione
- Contatti dei tecnici
- Indirizzo IP del name server che gestisce il dominio

- Queste info sono inserite nel database **WhoIs**
- Questo database è di pubblico accesso e fornisce "an important resource to Internet users including registrants, registrars, businesses, ISPs, intellectual property holders, and governmental law enforcement and consumer protection agencies."

  VEDI: <http://www.icann.org/riodejaneiro/whois-topic.htm>

Registrare un nome di dominio: quale livello?

- I suffissi (corrispondenti ai TLD) sono regolati dalla *Domain Name Authority* (ICANN) e sono relativamente stabili, sebbene i fermenti degli ultimi anni porteranno a molto più dinamismo
- **Quindi, una tipica organizzazione può scegliere il nome desiderato di secondo livello (SLD)**
  - Il nome deve essere unico all'interno di un TLD
  - Vi sono nomi soggetti a leggi internazionali per trademark, copyright, ecc.
  - Può scegliere:
    - Contratto indiretto (tramite un Registrar)
    - Contratto diretto con Registration Authority se ha le competenze

Due tipi di contratto con ccTLD “it”

- **Contratto Maintainer**

  Per le aziende che intendono registrare nomi a dominio per conto terzi. Accreditate italiane più note:

  - **Aruba.it**
  - **Register.it**
  - **Tuonome.it**

- **Contratto diretto** (per Maintainer di se stessi)

  “Questo contratto sottintende appropriate competenze tecniche per la gestione del nome a dominio richiesto”

  - Checklist di competenze tecniche
  - Disponibilità di server failure independent
  - Lettera di assunzione di responsabilità

Registrare un nome di dominio

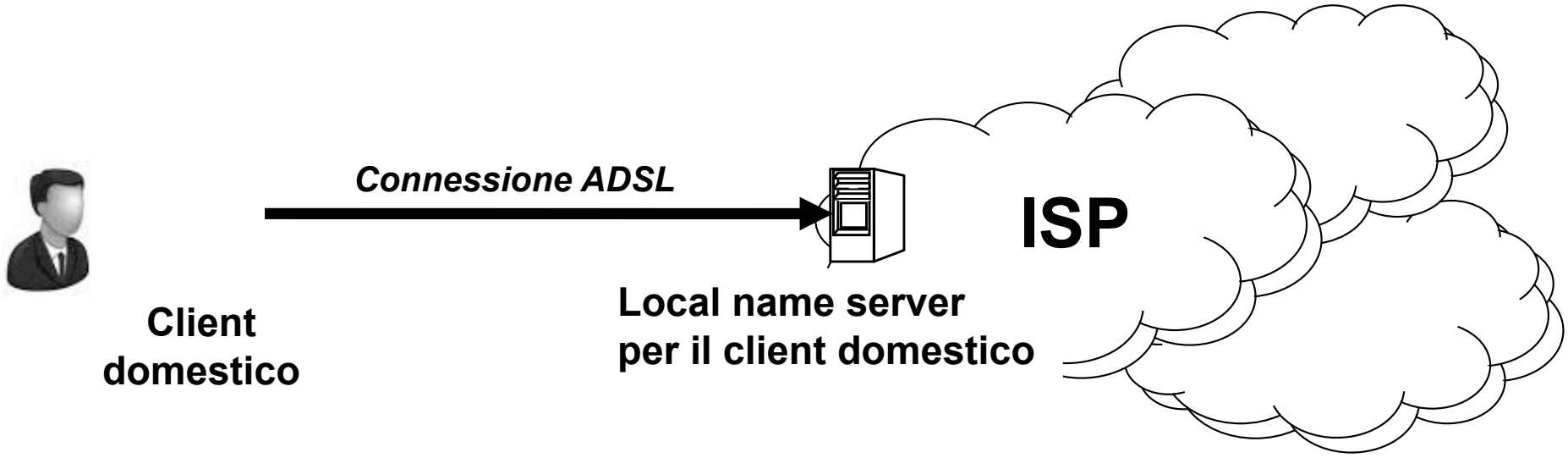
- Si supponga che l'organizzazione Jolly Inc. voglia registrare il dominio "**jolly.com**"
- Jolly Inc. è il ***registrant*** che si rivolge tipicamente ai servizi di un ***registrar***.
- Jolly Inc. deve prima verificare che il nome di dominio scelto sia ancora disponibile (nell'ambito di quel TLD .com)
- Se è disponibile, può registrare il dominio scelto:
  1. Per un periodo di tempo limitato, per esempio 2 anni
  2. Pagando una quota che dipende dal registrar
  3. Fornendo **"contact information"** (che andranno nel database **whois**)

Local name server: varie possibilità

1. **Client di organizzazioni senza dominio**
2. **Dominio delegato** (*Contratto indiretto*)
3. **Dominio gestito** (*Contratto diretto*)
   - 1 zona (organizzazioni di medie dimensioni in termini di numero di host)
   - Più di 1 zona (organizzazioni di grandi dimensioni, inclusa Università)
4. **Uso di local DNS pubblici**

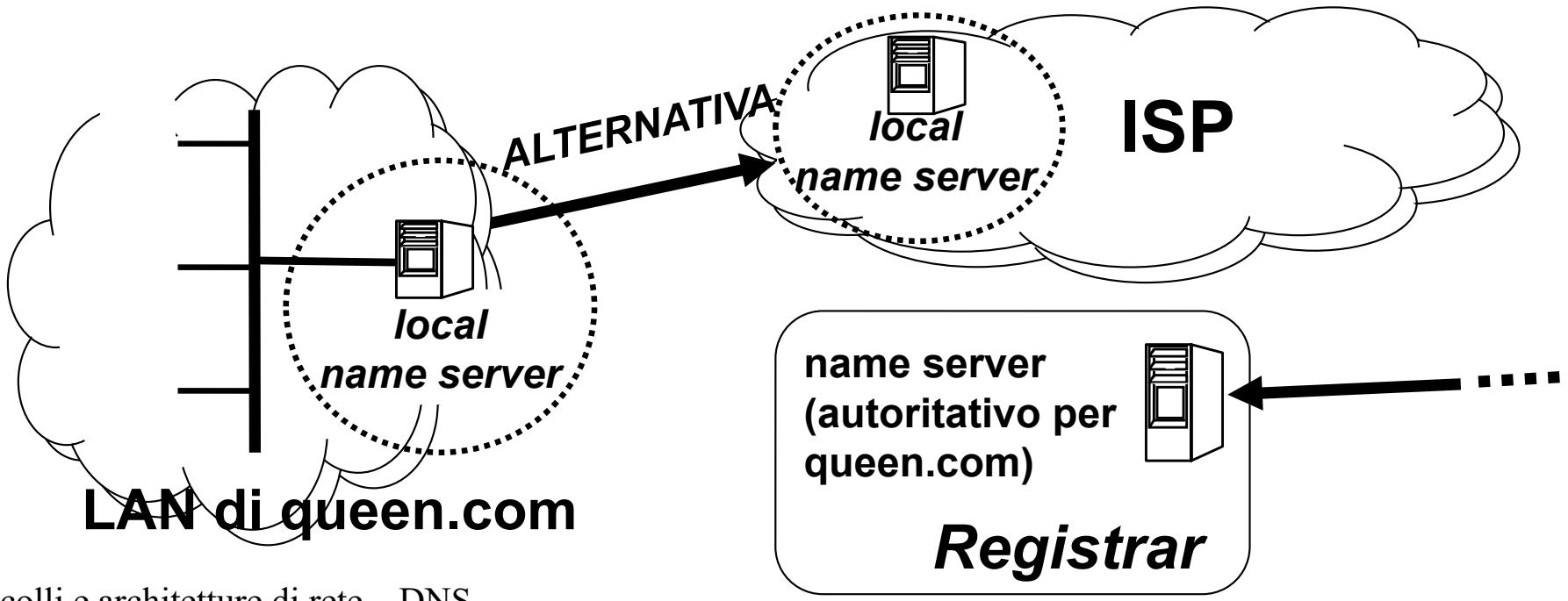
Tipo 1: client domestici o di organizzazioni senza dominio

- Le cosiddette utenze SO-HO (Small Office – Home Office) che non appartengono ad alcun dominio registrato delegano le funzioni di ***local name server*** al proprio ISP
- L'ISP che gestisce un Point-of-Presence (POP) offre, oltre alla connettività, un ***servizio DHCP*** mediante il quale si configura automaticamente sia l'IP del client sia il suo local name server
- Non essendovi dominio, non vi è *authoritative name seerver*



Tipo 2: client di organizzazioni con dominio delegato

- Le organizzazioni con dominio registrato (es., **queen.com**) con **contratto indiretto** mediante un provider detto "**registrar**" (es., Aruba) delegano a questa società la gestione dell'*authoritative name server* per il dominio **queen.com**
- La società proprietaria del dominio queen.com può gestire un local name server oppure delegare tale funzione a un name server del proprio ISP: è una scelta dell'azienda e dell'amministratore di rete



Tipo 3: client di organizzazioni con dominio gestito direttamente

- Organizzazioni più grandi che hanno in gestione un dominio (es., king.com) con “contratto diretto” tipicamente gestiscono anche:
  - un proprio ***name server autoritativo*** per il dominio king.com
  - uno o più ***local name server***