DNS o Domain Name System è un protocollo di livello 5 e si occupa della gestione degli hostname.

> è un sistema perché include il modello dei nomi

Gestisce i nomi al posto degli indirizzi (che invece vengono usati dalle macchine) perché devono essere comprensibili agli umani

- Questo è un sistema scalabile --> è adatto per tutto internet, senza introdurre colli di bottiglia.

Identificatori

Ogni dispositivo può essere identificato (oltre grazie all'indirizzo ip) con un **Hostname**, un nome utilizzato dagli utenti (ovvero una stringa alfanumerica di al più 255 caratteri). È una struttura gerarchica di **label** separate dal carattere `.`:

- ogni label deve essere di almeno 1 carattere e di al più 63
  - I caratteri consentiti sono IDN, un sottogruppo di UNICODE

> non esiste un vincolo fra IP e hostname

L'odine di *gerarchia* è inverso rispetto all'indirizzo IP --> si parte da **destra** e scorrendo ci dice in maniera gerarchica dove è l'host

```
sun3.dii.ing.unimore.it
```

- `.it` --> Country code
- `.unimore` --> solitamente il nome dell'organizzazione
- `.ing` --> interno

Questo è un `Hostname FQDN` (Fully qualifide domain name) o **canonico**, questo è formato da:

- `sun3` --> chiamato hostname relativo o semplicemente **hostname**
- `dii.ing.unimore.it` --> chiamato **Dominio** risulta quindi che:

```
FQDN = hostname.Dominio
```

I nomi possono essere anche utili perché rimangono "statici", mentre gli IP potrebbero cambiare. Facendo ciò però ovviamente si aggiunge un Layer per il LookUp:

- LookUp --> trasformazione da hostname a indirizzo
- Reverse LookUp --> trasformazione da indirizzo a nome

Terminologie

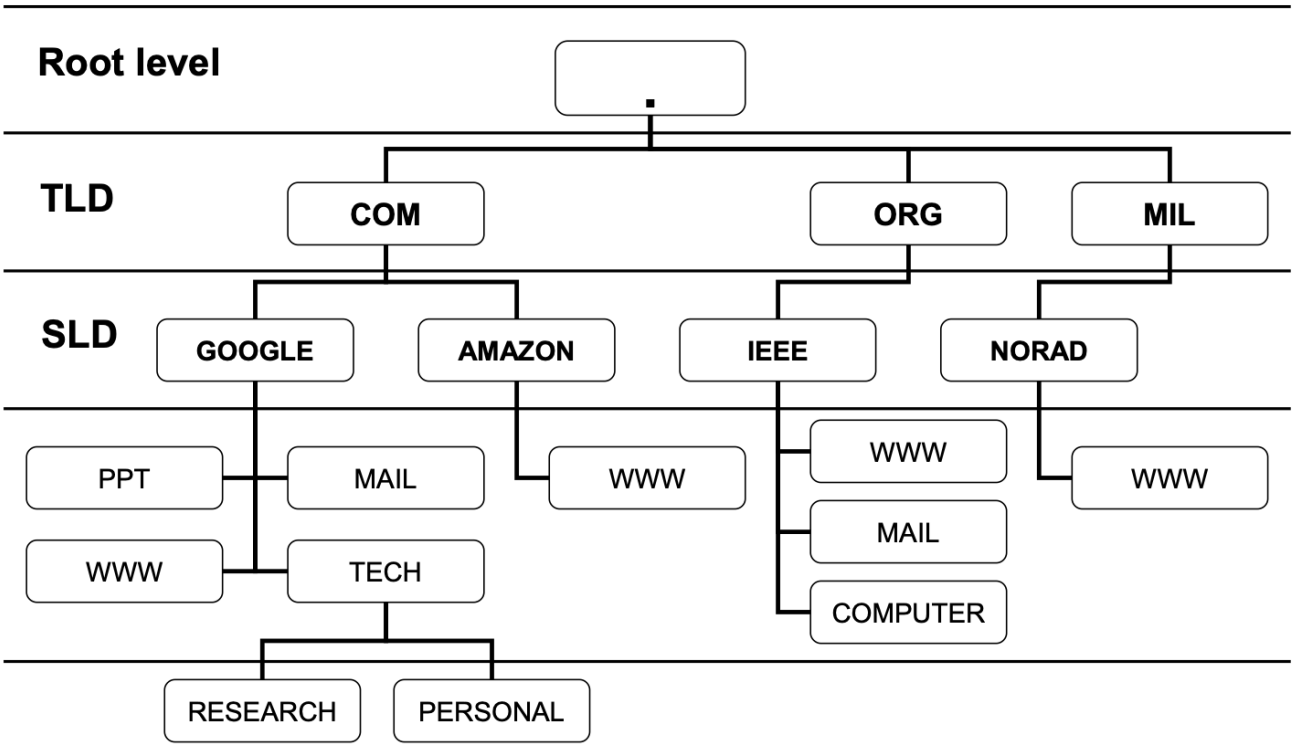
- la parte iniziale (nell'esempio `.it`) prende il nome di `Top Level Domain Name` --> di solito identifica dove è gestito (il paese) o lo scopo del servizio
- la parte subito prima (nell'esempio `.unimore`) prende il nome di `Second Level Domain Name` --> associato solitamente all'organizzazione

TLD

Esistono differenti tipologie di Top Level Domain Name, una volta in base allo scopo, ora non necessariamente vero:

- gTLD -->generic TLD, associati a uno scopo (.com . edu ...)
- ccTLD --> country code TLD, è associato a un paese
- iTLD --> infrastructure TLD (.arpa) --> non utilizzabile, host tecnici

Si può rappresentare la gerarchia dei domini con una radice unica: tutti i TLD sono figli della `root`



Architettura

Implementa un meccanismo efficiente per risolvere HOSTNAME:

- ci sono molteplici **Nameserver** che gestiscono LookUp e R-LookUp
- È un sistema distribuito, non esiste un server centrale, ma allo stesso tempo non sono indipendenti, esiste un gestore di **delega di risoluzione**, nessuno ha tutti i nomi
- uso di chacing a tutti i livelli
- utilizza UDP per LookUp e R-LookUp --> vengono anche utilizzati TLS-HTTPS

Classi di Nameserver

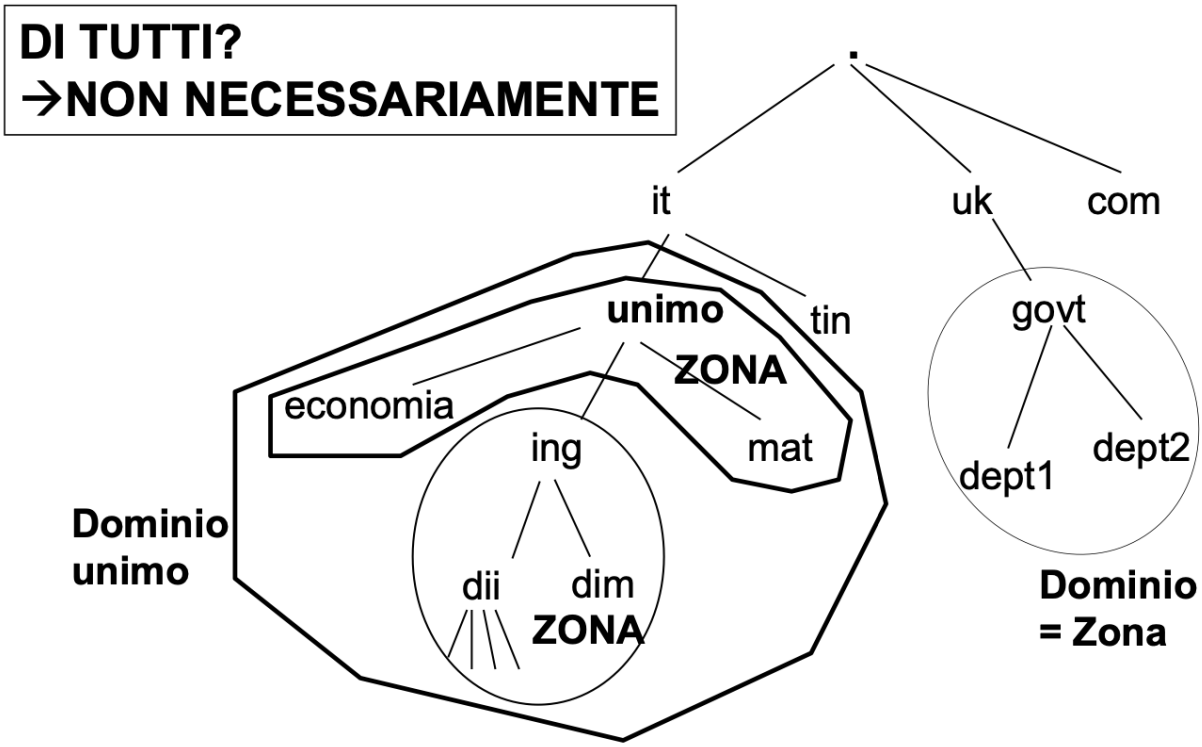
- Root name server (.) -> radice

- TLD name server --> relativi ai domini top-level

Esistono numerosi ROOT name server, sincronizzati, che gestiscono la delega verso i TLD. I Root name server indirizzano il traffico ai name server del TLD (almeno 1 per TLD), che gestiscono i dati e le richieste relative ai gTLD e ai ccTLD. Questi devono registrarsi sui Root name server.

> Questa modalità viene propagata gerarchicamente al di sotto dei nameserver

Ogni name server non ha i dati di tutti i nomi, ma sono responsabili di una **zona**



Non si è obbligati a introdurre un name server per ogni sotto dominio --> si può dire che un name server deve avere informazioni su gerarchie differenti, per esempio può scavalcare i sotto domini --> es il server si potrebbe occupare anche dei domini i ING senza far appoggio su un ulteriore name server

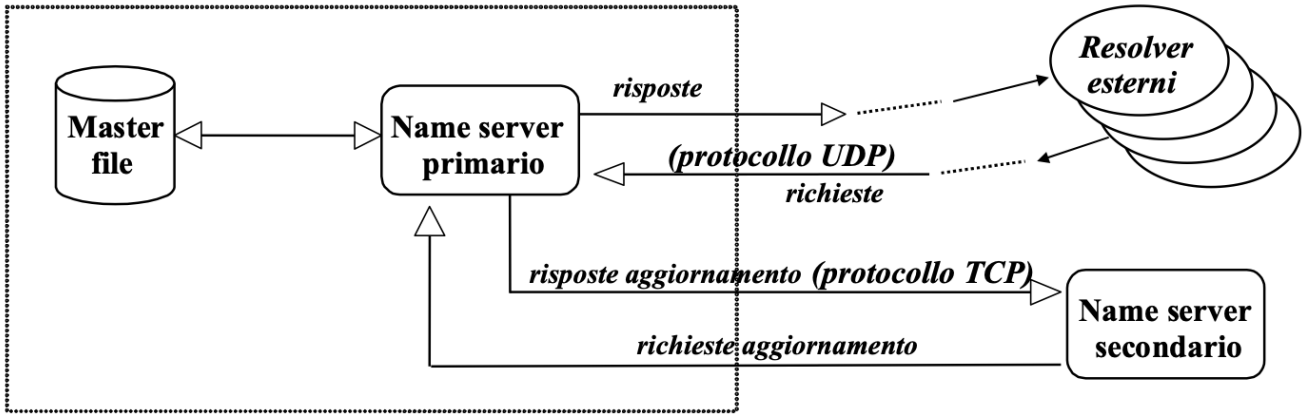
Generalemente gli amministratori di sistema inseriscono i dati relativi ad una Zona in un **master file** che è l'unica sorgente di *dati autoritativi* per quella Zona. Esistono due tipi di name server che possono fornire *dati autoritativi*:

- **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

Per garantire che i dati su hostaname e indirizzi IP di una Zona siano disponibili anche quando un name server fallisce, le specifiche dell'architettura del DNS richiedono che ogni Zona debba essere replicata in **almeno due server autoritativi** che siano tra di loro *failure indipendent*

Aggiornamento e consistenza

I name server che hanno informazioni su di una stessa Zona vengono distinti in **name server primari (master)** e **name server secondare (slave)**. Nel name server primario possono essere effettuate modifiche sui nomi della zona. Il mantenimento della consistenza del database è effettuato dai name server secondari che periodicamente interpellano il server master per controllare eventuali cambiamenti



Tipi di Resource Record

I name server sono di fatto dei database distribuiti che contengono record su:

- Zone
- Indirizzi
- Gestione server
- `...` Ci sono decine di tipi di resource record, anche se solo pochi sono utilizzati comunemente, ecco i principali:
- `A` --> Record che mappa Host address e indirizzo IP, include l'associazione fra hostname canonico e indirizzo IP di un host
- `NS` --> Record che descrive il name server autoritativo per una determinata Zona --> mappa dominio e name server
- `SOA` (**Start Of Authority**) --> Record che descrive i parametri relativi alla gestione della Zona
- `MX` (**Mail Exchanger**) --> Record relativo a un server che gestisce email per un determinato dominio (simile ad A, ma cambia il contesto)
- `CNAME` --> Record che mappa hostname a hostname: canonical name per un alias. Un host può avere più hostname di cui uno canonico e altri definiti alias. un Cname non può contenere indirizzi IP
- `HINFO` --> Host information
- `AAAA` --> Uguale ad A però per IPv6

Ciascun RR ha un TTL --> per quanto tempo quell'informazione è valida, questo fa si che si evitino query DNS su uno stesso indirizzo. Se questo campo è a 0 significa che il name server va sempre consultato.

Local Name server

Ogni organizzazione e ogni provider (ISP) gestisce uno o più name server locali: questi sono le foglie dell'albero dei name server. Il name server locale:

- È configurato dal client
- È fornito automaticamente in un contesto DHCP I suffissi (corrispondenti al TLD) sono regolati dal **Domain Name Authority** (ICANN) e sono relativamente statici. 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:
  - contatto indiretto --> tramite un **Registrar** ovvero una società intermedia autorizzata che fornisce servizi di registrazione
  - contatto diretto --> con Registration Authority se ha le competenze

Meccanismo distribuito di risoluzione dei nomi

Premesse:

- 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 attivata dalla componente *Resolver* del client

Resolver

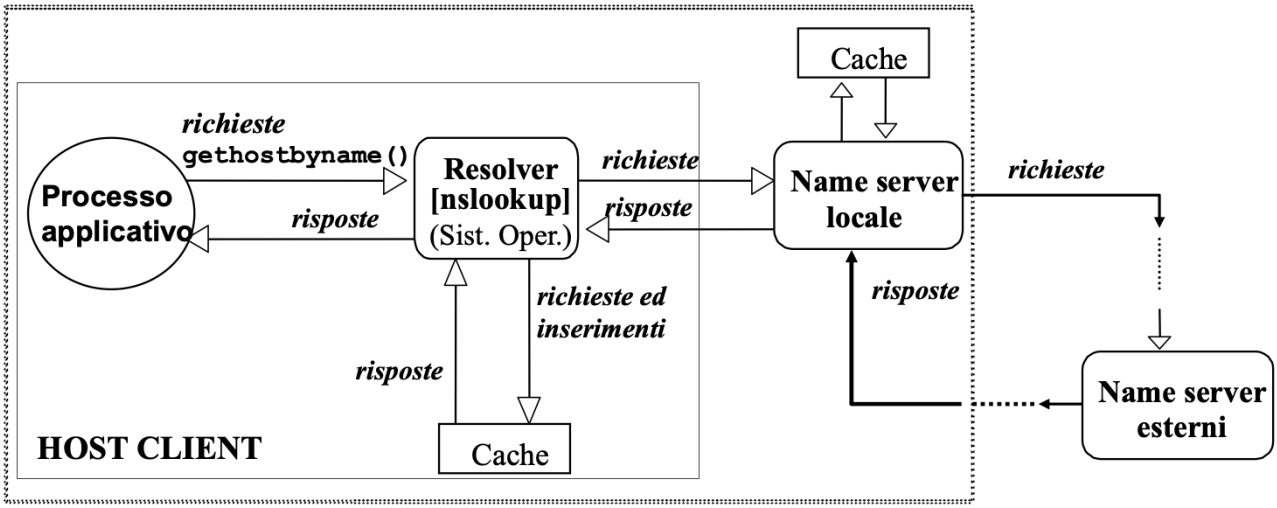
I Resolver sono i primi client del sistema DNS che sottomettono query al loro *local name server* per risolvere indirizzi su hostname e indirizzi IP per conto delle applicazioni Internet. Ogni Resolver deve conoscere il riferimento ad almeno un name server locale

Tipi di Query

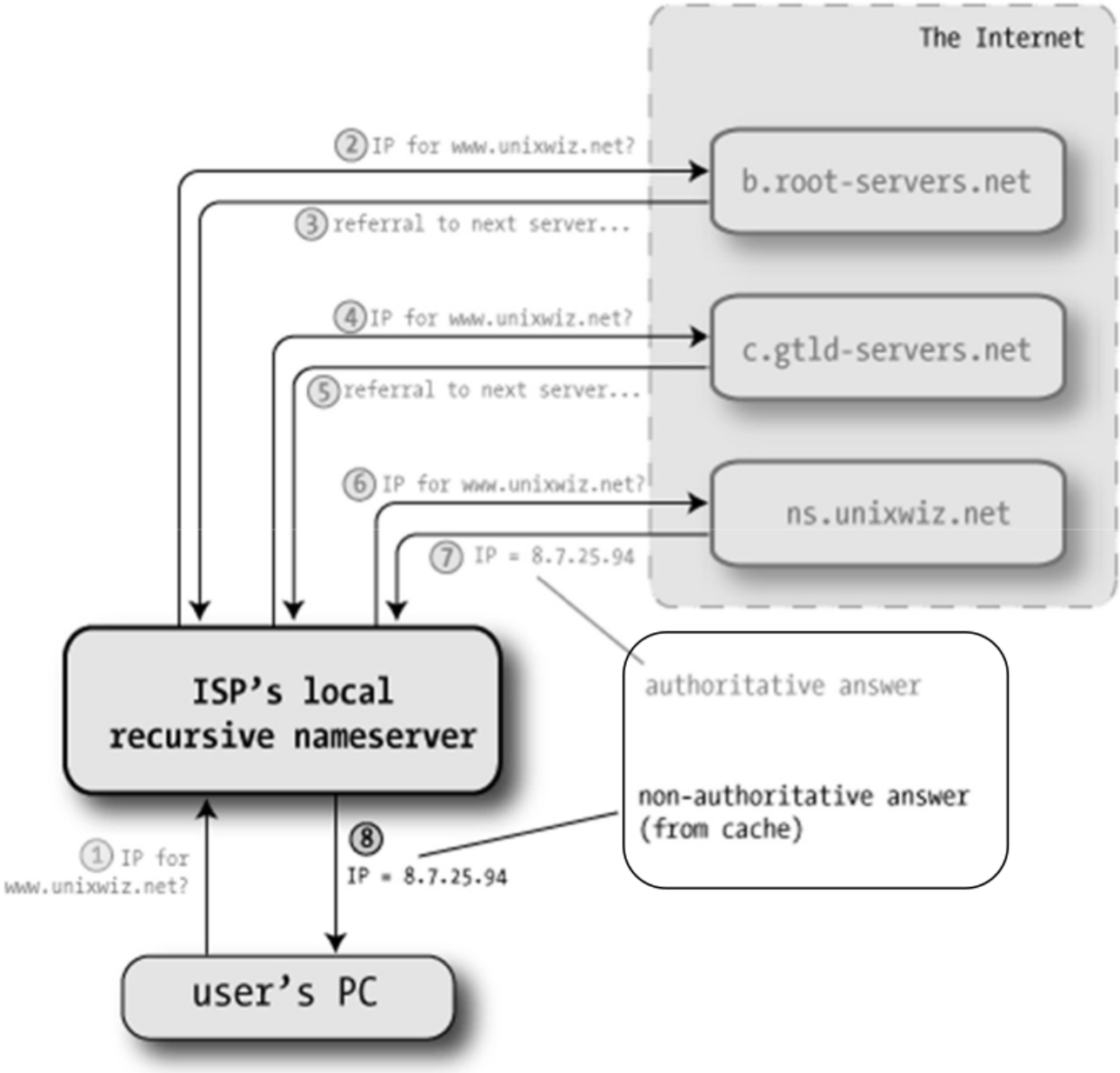
Ciascun name server può essere configurato per rispondere a due tipologie di query nella risoluzione di un nome:

- **Query ricorsiva** --> il server, contattato e non in grado di risolvere il nome richiesto, assume il ruolo di client nei confronti di un altro 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 solamente a query iterative, mentre i local name server tipicamente per query ricorsive



Ecco un esempio:



Chacing

Per ridurre i tempi di risposta, ogni name server del DNS è libero di effettuare chaching dei dati relativi ad altri serve ed altre zone in modo da evitare di contattarli quando una risoluzione viene richiesta più volte (i client vengono informati se una richiesta è stata presa dalla chace)

DNSSEC Estensione di sicurezza

DNS può soffrire di un problema di autenticità dei record che otteniamo dalle nostre query. Motivazioni:

- uso intensivo di intermediari:
  - local name server che effettua query ricorsive "al posto nostro"
  - uso intensivo di chaching

DNSSEC è una estensione di DNS che prevede l'impiego di **firme digitali** per garantire l'autenticità del record ricevuto