



DNS



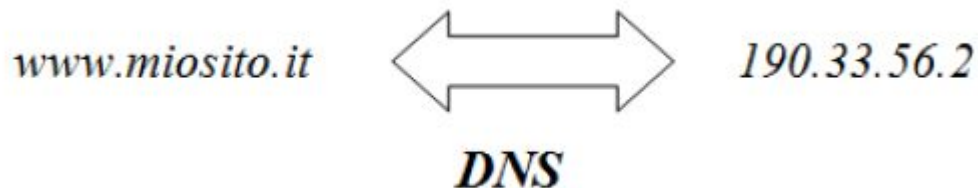
prof.ssa Denise Panarotto

# Protocollo DNS

---

Il **Domain Name System (1983)** è un protocollo di livello applicativo con cui l'utente generalmente non interagisce direttamente, ma viene utilizzato da altri protocolli come HTTP, FTP, SMTP per risolvere i nomi di dominio in indirizzi IP e viceversa.

Il DNS a livello di trasporto utilizza l'**UDP** e indirizza la **porta 53**.



# DNS Namespace

---

Il DNS utilizza uno schema delle denominazioni con struttura gerarchica, basato su domini e su un database distribuito di server.

Un nome di dominio è costituito da una serie di stringhe separate da punti, ad esempio it.wikipedia.org.

In un nome DNS, il dominio più significativo si trova all'estrema destra ed è detto **dominio di primo livello** (o TLD, Top Level Domain), per esempio .org o .it.

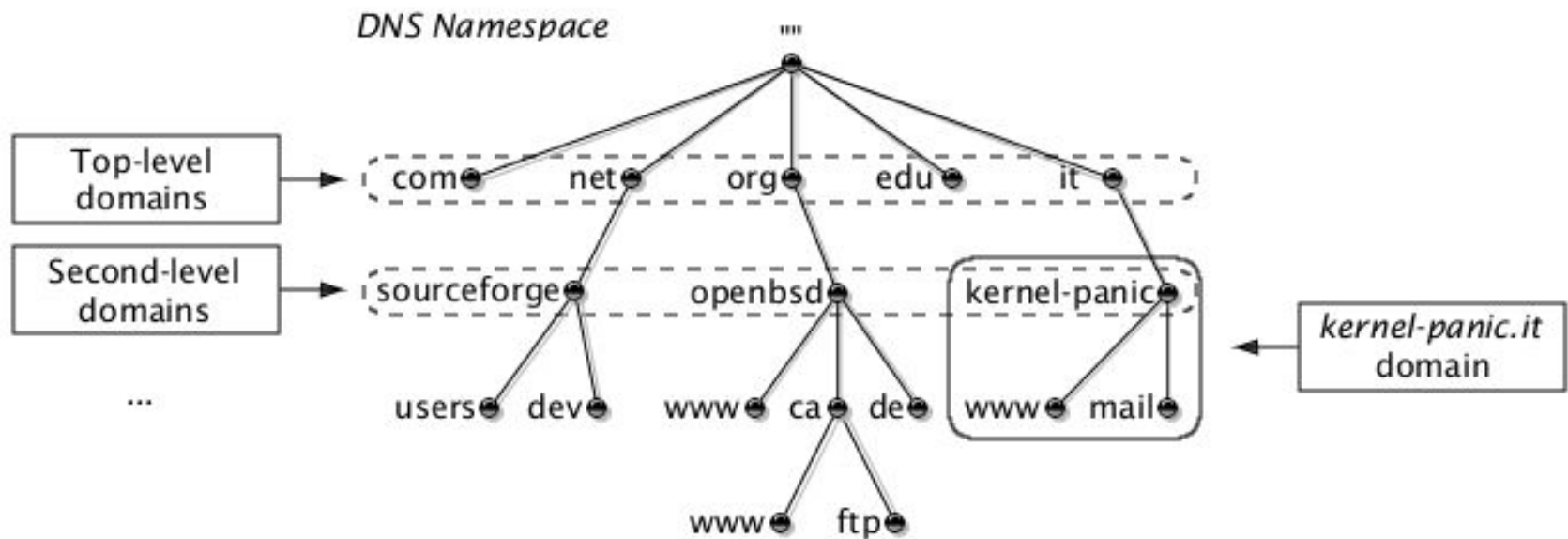
Un **dominio di secondo livello** consiste di due parti, per esempio wikipedia.org, e così via.



# DNS Namespace

---

Internet è divisa in oltre 250 domini di primo livello o **top level domain** (*generici* come edu, com, org...o *nazionali* come it, nl, uk...). Essi a loro volta si suddividono in *sottodomini di secondo livello*.... per cui è possibile utilizzare una rappresentazione ad albero. Il nome di dominio si costruisce partendo dalle foglie e risalendo verso la radice e si utilizza come separatore il *dot*.



# DNS domainspace

---

- a ciascun nodo dell'albero corrisponde un dominio e alle foglie corrispondono le risorse (es. web server) alle quali viene associato il nome
- I domini di primo livello detti TLD (Top Level Domain) possono essere distinti in:
  - **generici o gTLD**, questi si dividono ulteriormente in
    - sTLD (sponsored)
    - uTLD (unsponsored)
  - **nazionali o ccTLD** (country code TLD)
  - Dominio inverso: in-addr.arpa (un dominio speciale per la risoluzione inversa: address-to-name mapping)

In Italia l'assegnazione dei nomi di primo livello con dominio .it viene gestita da **Registro** (<https://www.nic.it/it>) che è responsabile della gestione del name server “.it”.

Il Registro è l'anagrafe dei domini Internet .it, la targa Internet dell'Italia. Soltanto qui è possibile chiedere, modificare o cancellare uno o più domini .it.

Registrar : <https://www.nic.it/it/registrar>

Mappa dei root server: <https://root-servers.org/>



# DNS domain space

---

gTLD			
sTLD		uTLD	
.edu	per i siti di educazione scolastica superiore	.com	per le organizzazioni commerciali
.gov	siti governativi	.net	infrastrutture di rete
.museum	musei	.org	organizzazioni
.asia	comunità dell'ASia	.info	siti informativi

ccTLD	
.it	Italia
.en	Inghilterra
.fr	Francia
.za	Sud Africa



# Gerarchia di dominio

---

Quando un dominio di secondo livello viene registrato all'assegnatario, questo è autorizzato a usare i nomi di dominio relativi ai successivi livelli come `it.wikipedia.org` o `en.wikipedia.org` (dominio di terzo livello) e così via per i livelli successivi.

I nomi di dominio sono soggetti a determinate **restrizioni**: per esempio ogni parte del nome (quella cioè limitata dai punti nel nome) non può superare i 63 caratteri e il nome complessivo non può superare i 255 caratteri.

Si definisce **Fully Qualified Domain Name (FQDN)** un nome di dominio che include tutti i domini di livello superiore al suo.

---



# Gerarchia di dominio

---

Il sistema DNS è costituito da migliaia di sever DNS presenti in rete che gestiscono un database distribuito con le informazioni riguardanti **i nomi di dominio** che identificano in modo univoco ciascuna risorsa presente in Internet (ad es. i nomi che consentono di raggiungere i server dei siti web).

Ognuno di questi server è responsabile di una certa porzione del nome, detta dominio.

**I server sono organizzati secondo una struttura gerarchica** così come **i nomi di dominio appartengono ad uno spazio gerarchico dei nomi.**

---





# Organizzazione dei server

---

Il mapping ( corrispondenza ) per tutti gli host di Internet viene distribuito su più server in modo gerarchico. I server vengono classificati in **3 gruppi**:

- ▣ **Root name server** : contengono l'elenco dei server responsabili dei domini di primo livello TLD ( [link](#) )
- ▣ **Top level domain ( TLD ) server**
- ▣ **Authoritative server**

Ci possono essere anche **server DNS locali** che interagiscono direttamente con le applicazioni

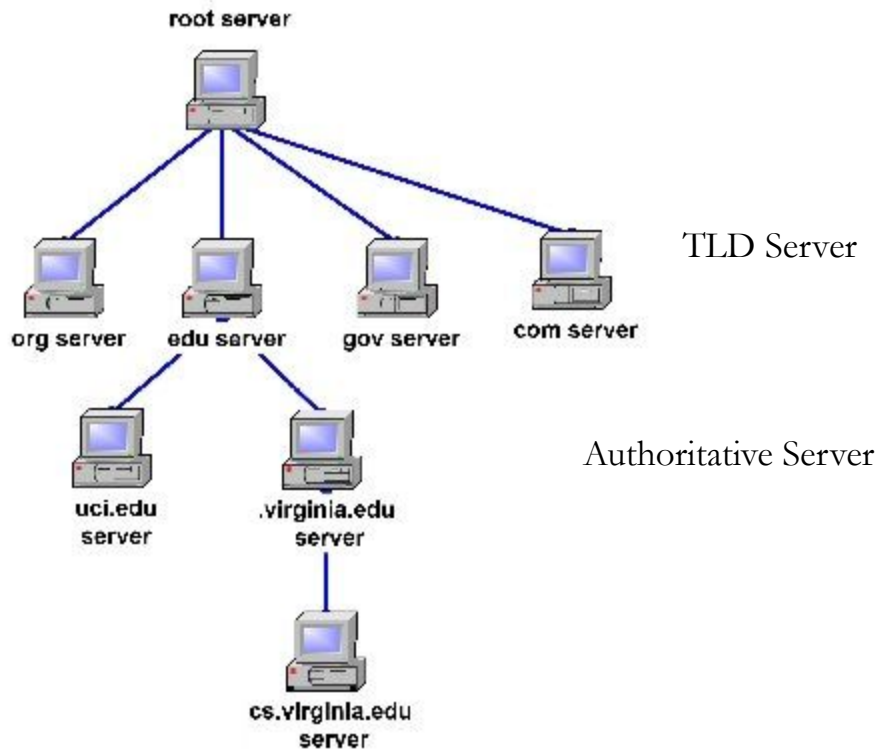


# Organizzazione dei server DNS

---

## Hierarchy of Name Servers

- ❑ The resolution of the hierarchical name space is done by a hierarchy of name servers
- ❑ Each server is responsible (authoritative) for a contiguous portion of the DNS namespace, called a **zone**.
- ❑ Zone is a part of the subtree



## DNS ROOT SERVERS

Nome host	Indirizzo IP	Gestore
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	<a href="#">VeriSign, Inc.</a>
b.root-servers.net	199.9.14.201, 2001:500:200::b	<a href="#">University of Southern California (ISI)</a>
c.root-servers.net	192.33.4.12, 2001:500:2::c	<a href="#">Cogent Communications</a>
d.root-servers.net	199.7.91.13, 2001:500:2d::d	<a href="#">University of Maryland</a>
e.root-servers.net	192.203.230.10, 2001:500:a8::e	<a href="#">NASA</a> (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	<a href="#">Internet Systems Consortium, Inc.</a>
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	<a href="#">US Department of Defense</a> (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	<a href="#">US Army</a> (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	<a href="#">Netnod</a>
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	<a href="#">RIPE NCC</a>
l.root-servers.net	199.7.83.42, 2001:500:9f::42	<a href="#">ICANN</a>
m.root-servers.net	202.12.27.33, 2001:dc3::35	<a href="#">WIDE Project</a>

*As of 2018-07-09, the root server system consists of 929 instances operated by the 12 independent root server operators. The 13 root name servers are operated by 12 independent organisations.*



# Resource Record

---

Quando un resolver sottopone un nome di dominio a un server DNS, ottiene come risposta i record delle risorse ad esso associate.

Associato ad un nome di dominio possiamo trovare più RR (Resource Record, cioè di un descrittore di risorsa) , ciascuno contenente informazioni di vario tipo (IP, nome di un altro server...)

Un **RR** è costituito dai seguenti campi:

*<Name, Value, Type, Class, TTL>*

dove :

- ▣ **Name:** nome fornito al DNS in input
- ▣ **Value:** valore restituito dal DNS in output
- ▣ **Type:** indica come va interpretato il valore memorizzato nel RR
- ▣ **Class:** indica la classe di appartenenza del RR (IN=Internet)
- ▣ **TTL** (Time To Live): per quanto tempo è valido il contenuto di RR, quando scade il tempo il record viene eliminato



# RR Type

---

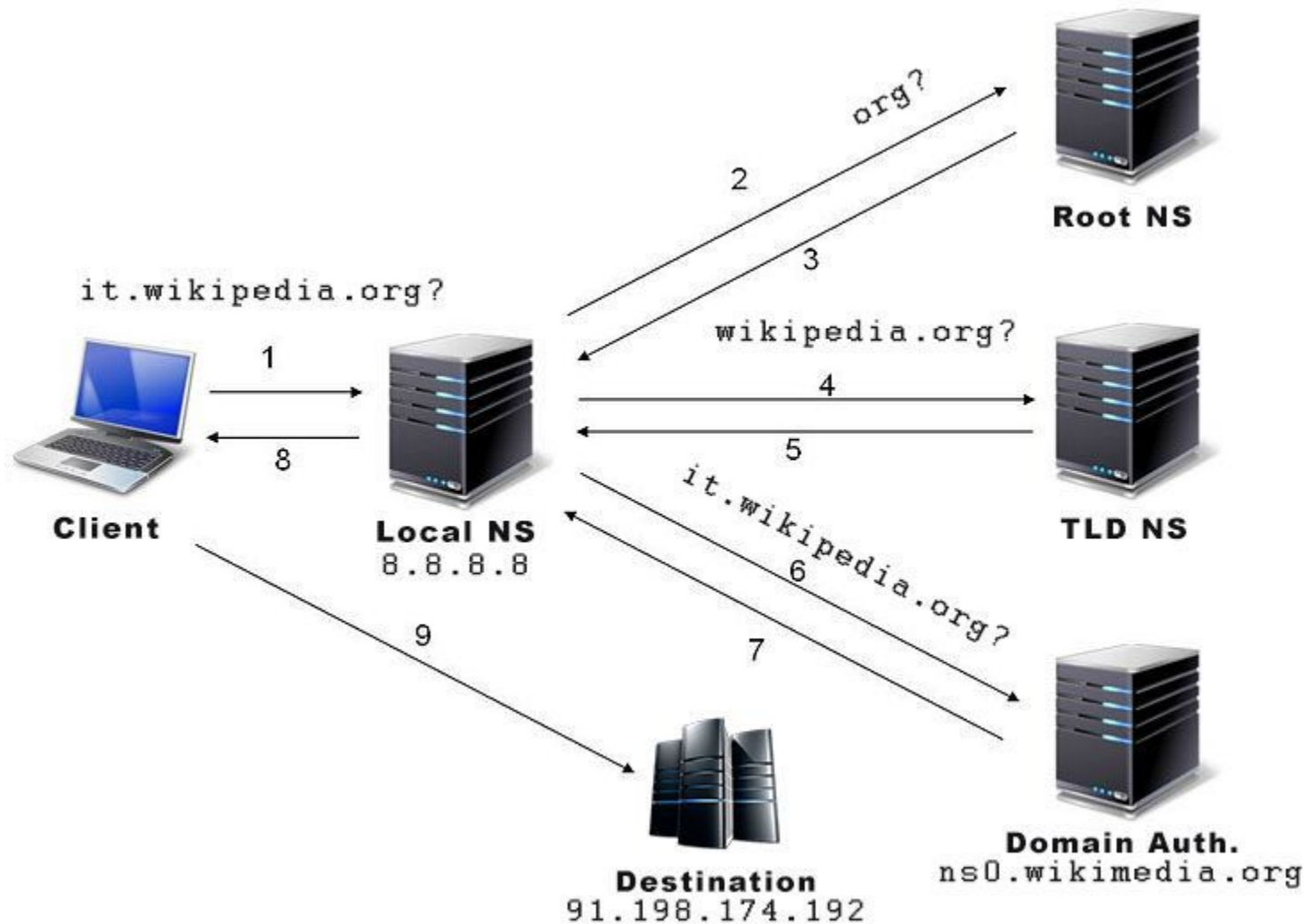
Type=A	Indirizzo IPv4 del dispositivo
Type=MX	Mail eXchange record: nome di dominio del server di posta elettronica
Type=NS	authoritative Name Server: nome di dominio del calcolatore che sa risolvere i nomi per il dominio specificato
Type=CNAME	canonical name: è utilizzato per definire nomi alternativi, alias di una risorsa/computer
Type=AAAA	indirizzo IPv6

Il root server contiene una coppia di record uno con Type=A ed uno con Type= NS per ciascun server di primo livello. Questa coppia di record consente di individuare i TLD server i quali a loro volta avranno le coppie di record A ed NS che individuano i server di secondo livello...fino ad arrivare al server che contiene il solo record A che risolve il nome di dominio richiesto.

---



# Interrogazione del DNS (iterativa)



## Interrogazione del DNS (iterativa)

---

**Ogni ISP ha un local name server.** La richiesta di un client viene prima inoltrata a questo server il quale consulta la propria cache memory per vedere se ha già la risposta, altrimenti inoltra la richiesta ad un root name server che restituirà l'elenco dei TLD che gestiscono il dominio interessato. Il local name server dell'ISP contatta uno di questi server per arrivare ad ottenere la risposta cercata come indicato nella figura precedente.

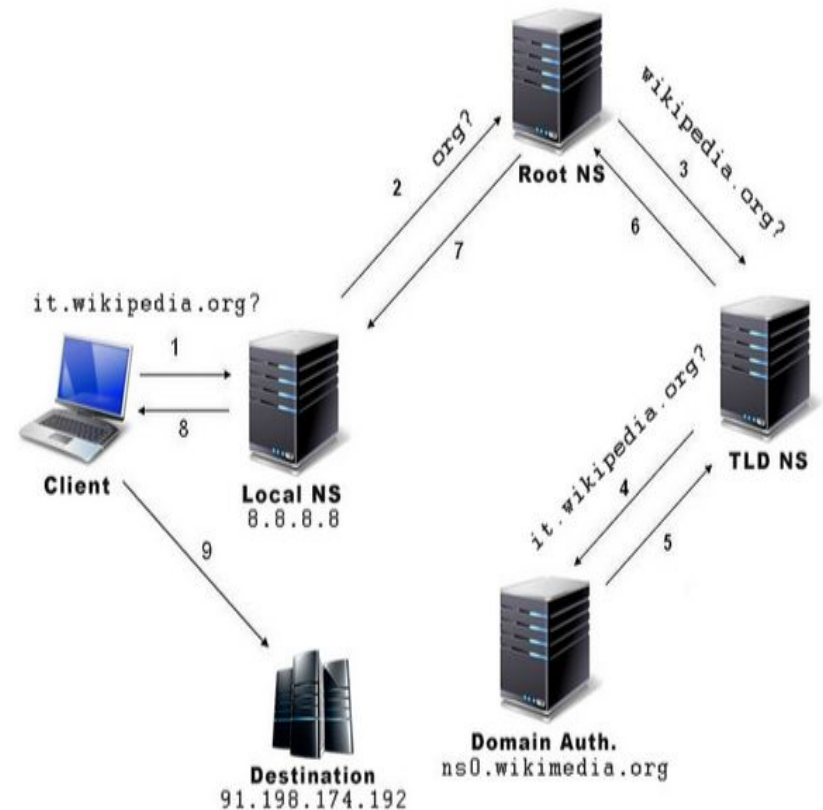




# Interrogazione ricorsiva

1. Il **client** chiede al **Local NS** l'indirizzo del dominio;
2. Il **Local NS** delega la richiesta al **Root NS**;
3. Il **Root NS** delega la richiesta al **TLD NS**;
4. Il **TLD NS** interroga il **NS autoritativo** per il dominio;
5. Il **NS autoritativo** rimanda il record al **TLD NS**. Il record viene passato tra tutti i **NS** coinvolti, fino al **Local NS**;
6. Il **Local NS** restituisce l'indirizzo al **client**, che raggiunge la **destinazione**.

I **NS** sono interrogati **ricorsivamente**. Ogni NS coinvolto, **interroga il successivo**, che interrogerà quello successivo ancora.





# Servizio Client su Windows

---

- ❑ Comando per vedere le voci DNS presenti nella cache del proprio dispositivo:  
**ipconfig /displaydns**
- ❑ comando per svuotare la cache  
**ipconfig /flushdns**
- ❑ comando per interrogare il server DNS e recuperare i nomi di dominio tramite un DNS specifico:  
**nslookup [www.cern.org](http://www.cern.org) 8.8.8.8**  
**nslookup www.google.com ns1.google.com**

oppure tramite il DNS di default:

**nslookup [www.cern.org](http://www.cern.org)**

---



## Link Esempi

```
C:\Users\dpana>nslookup -type=A it.wikipedia.org
Server:  UnKnown
Address:  2001:b07:ad4:1bfe::1
```

Risposta da un server non autorevole:

```
Nome:      dyna.wikimedia.org
Address:   91.198.174.192
Aliases:   IT.wikipedia.org
```

risposta da un server  
non autorevole

```
C:\Users\dpana>nslookup -type=NS it.wikipedia.org
Server:  UnKnown
Address:  2001:b07:ad4:1bfe::1
```

Risposta da un server non autorevole:

```
it.wikipedia.org      canonical name = dyna.wikimedia.org
```

wikimedia.org

```
primary name server = ns0.wikimedia.org
responsible mail addr = hostmaster.wikimedia.org
serial  = 2021121620
refresh = 43200 (12 hours)
retry   = 7200 (2 hours)
expire  = 1209600 (14 days)
default TTL = 600 (10 mins)
```

Cerco un server  
autorevole ->  
ns0.wikimedia.org

```
C:\Users\dpana>ipconfig /flushdns
```

Configurazione IP di Windows

Cache del resolver DNS svuotata.

```
C:\Users\dpana>nslookup wikipedia.org ns0.wikimedia.org
Server:  ns0.wikimedia.org
Address:  208.80.154.238
```

```
Nome:      wikipedia.org
Addresses: 2620:0:862:ed1a::1
           91.198.174.192
```

mi rivolgo al server autorevole che  
mi ritorna IPv6 e IPv4 per  
wikipedia.org