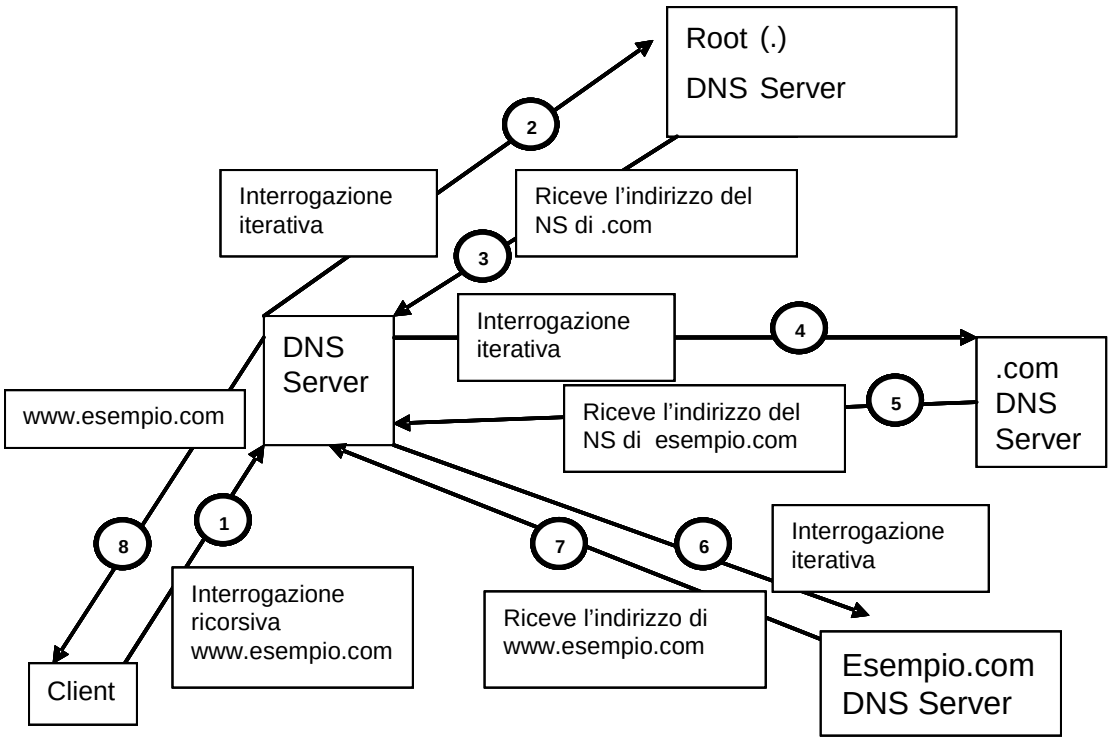
Un client che interroga un server DNS viene chiamato **resolver,** mentre un server DNS prende generalmente il nome di **Name Server (NS)**.
Il DNS lavora al livello applicativo (settimo livello) del modello OSI. In questo modo, il DNS può facilmente comunicare con l'applicazione client che vuole risolvere un hostname in un indirizzo IP o viceversa.
Il DNS usa per le proprie comunicazioni sia il l'UDP che il TCP (ad esempio per i *zone-tranfers*), rimanendo in ascolto sulla porta 53 per quanto riguarda il *server-side*.
Possono essere inoltrate ad un NS tre tipi di interrogazioni:

1. **Ricorsiva** – obbliga il NS interrogato a rispondere alla richiesta con una risposta che può essere positiva (risoluzione avvenuta) oppure negativa (risoluzione impossibile).
   Con un'interrogazione ricorsiva, il NS interrogato se non è in grado di rispondere direttamente, deve interrogare a sua volta un altro NS impegnandosi ad inoltrare l'eventuale risposta al resolver originario. E' necessario sottolineare che in questo modello di interrogazione, non è permesso che il NS interrogato dal resolver gli risponda con un *referral* ovvero con l'indirizzo di un altro NS, ma solo con una risposta finale.
   Quindi l'interrogazione ricorsiva avviene in due casi
   a. i **resolvers** si rivolgono ai propri Servers DNS aspettandosi da essi una risposta precis ed incontrovertibile.
   b. Un NS (*slave*) si rivolge al proprio **forwarder** preposto ad inoltrare le interrogazioni ricevute (tipicamente un NS di frontiera in comunicazione con una WAN a cui si rivolgono i NS interni ad una o più LAN)
2. **Iterativa –** la risposta attesa da parte del NS interrogato è quella possibile sulla base delle informazioni ad esso disponibili (file di zona o cache); in caso negativo il NS rimandan ad un altro NS che abbia "autorità" sul dominio in questione.
   La figura seguente mostra il comportamento degli attori coinvolti in un'interrogazione ricorsivo-iterativa per la risoluzione dell'indirizzo di www.esempio.com



Il NS che riceve l'interrogazione ricorsiva da parte del client non può risolvere direttamente l'hostname ricercato, quindi inizia un'interrogazione iterativa per recuperare l'informazione. Come prima cosa, contatta uno dei root NS (.) sparsi per il mondo il quale gli spedisce indietro il referral al NS con autorità sul dominio .com (*top-level domain*).
A questo punto, il NS del client continua con un'altra interrogazione iterativa, ma questa volta verso il NS del domimio .com, il quale gli risponde con l'indirizzo del NS sotto la cui autorità è il dominio esempio.com.
Finalmente, il NS può interrogare iterativamente il NS di esempio.com richiedendo la risoluzione di www.esempio.com, cosa che gli tornerà indietro come una risposta che a sua volta inoltrerà al resolver originario che nel frattempo ha atteso una risposta definitiva dalproprio NS, così come impone un'interrograzione ricorsiva.

3. **Inversa –** usata quando il resolver vuole conoscere l'indirizzo IP associato ad un certo *hostname*. Per ottimizare questo tipo di ricerca è stato creato uno speciale dominio chiamato **in-addr.arpa,** impedendo così che fosse necessario per il NS cercare attraverso tutti i domini fino a trovare quello giusto**.** I nodi appartenenti a questo spazio sono differenziati dal proprio indirizzo IP preso in ordine inverso; infatti, gli *hostnames* seguono una convenzione per cui da destra a sinistra si passa dal generale allo specifico (srv-1.supporto.esempio.com), quindi gli indirizzi IP per rappresentare lo stesso ordine devono essere invertiti (212.34.21.67 diventa 67.21.34.212.in-addr.arpa.)

Un NS può rispondere ad un'interrogazione in tre modi:

- Risposta positiva in caso di successo (indirizzo IP o hostname)
- Risposta negativa in caso di insuccesso
- Un puntatore (*referral*) ad un altro NS nel solo caso dell'interrogazione iterativa

Un NS che risponda al resolver con attingendo fuori dalla propria zona di autorità, pone nella propria cache tale risoluzione in modo da poterla efficientemente utilizzare nel caso venga nuovamente richiesta in futuro. Il tempo di durata di una risoluzione nella cache del NS è dato da un parametro chiamato TTL (Time-To-Live) che evita la possibilità che le informazioni vengano mantenute indefinitivamente ovvero che si abbiamo risoluzioni sbagliate in seguito ad un cambiamento dell'associazione tra hostname ed indirizzo IP risolti.
La scelta di un corretto valore del TTL implica alcune considerazioni aggiuntive:

- TTL di breve durata – utile nel caso in cui i cambiamenti nel database DNS avvengano in modo frequente, comporta però un maggior traffico DNS tra in NS fino al rischio di sovraccaricare la struttura.
- TTL di lunga durata – a fronte di un minore traffico DNS, esiste la possibilità che le risposte del NS siano non aggiornate rispetto alla realtà del database DNS e quindi si rivelino errate.

Il valore del TTL si propaga lungo la catena dei vari NS fino al resolver, ovvero nel caso in cui un primo NS riceva dalla cache di un secondo NS la risoluzione richiesta da un resolver, il secondo NS invia il TTL della risoluzione cachata al primo NS. Qust'ultimo assume il TTL ricevuto come proprio TTL e inoltrerà la risposta al resolver, il quale, avendo una propria cache per ottimizzare le risoluzioni a richieste già fatte in precedenza, porrà il TTL uguale a quello ricevuto dal proprio NS. Ciò server a mantenere una coerenza temporale della scadenza del TTL attraverso tutto l'albero gerarchico del DNS.