

DNS

Il DNS è il protocollo che trasforma il nome di dominio a l'indirizzo IP, è un'applicazione client - server. Questo è il primo passaggio per avere una ricerca in HTTP.

All'interno della sezione DNS del server, si può andare a impostare un Resource Records, ovvero una tabella suddiviso per:

- Name: ovvero il nome del dominio a cui il record appartiene
- Type: identifica il tipo di informazione contenuta nel campo RData
- Class: indica se le informazioni del record fanno riferimento a Internet o ad altro. La classe Internet è indicata con IN
- TTL: indica la stabilità del record, scaduto il TTL e si ha ancora il TTL = 0 in memoria, bisogna richiederlo
- RDLenght: Specifica la lunghezza in ottetti del campo RData
- RData: è il valore restituito dal DNS, può contenere un numero o una stringa ASCII

Esempio: pingu.di.school.it. A IN 86400 198.45.30.165

Il DNS si divide in 3 parti:

- Domini radice: la parte finale nostro indirizzo (.it / .com)
- Domini intermedi: sono i domini che hanno a loro volta sotto domini, ovvero tutta la parte dopo il "www" e prima del ".it / .com"
- Domini foglia: è la parte iniziale del nostro indirizzo "www. / young."
- Esempio: .it → denina → www.

Per il DNS valgono le seguenti regole:

- Nomi facili, che non devono superare i 63 caratteri
- Utilizzare meno di 5 livelli
- I nomi di *case-insensitive* è indifferente

- Ogni dominio controlla il suo sotto dominio

DNS (Domain Name System):

Il Domain Name System (DNS) è un sistema di gerarchia distribuito utilizzato per tradurre nomi di dominio, come www.example.com, in indirizzi IP, come 192.0.2.1. Il DNS è fondamentale per consentire agli utenti di utilizzare nomi di dominio comprensibili invece di dover memorizzare indirizzi IP numerici.

Formato dei pacchetti DNS:

I pacchetti DNS contengono diverse sezioni, tra cui:

1. **Header:** Contiene informazioni come identificatore, flag di controllo, numero di domande, risposte, autorizzazioni, ecc.
2. **Domande (Questions):** Una o più domande DNS.
3. **Risposte (Answers):** Una o più risposte che contengono i record richiesti.
4. **Autorizzazioni (Authority):** Informazioni autoritative sulla zona DNS, come i server dei nomi autorizzati per il dominio.
5. **Altri informazioni (Additional):** Informazioni aggiuntive, ad esempio i server DNS autorizzati.

Resource Record (RR):

I record delle risorse (Resource Records o RR) sono elementi di dati all'interno di un pacchetto DNS e contengono informazioni specifiche su un dominio. Alcuni tipi comuni di RR includono:

- **A:** Mappa un nome di dominio a un indirizzo IPv4.
- **AAAA:** Mappa un nome di dominio a un indirizzo IPv6.
- **CNAME:** Specifica un nome di dominio canonico (alias) per un altro nome.
- **MX:** Definisce il server di posta responsabile per il dominio.

- **NS:** Specifica i server dei nomi autorizzati per un dominio.

Come funziona il DNS:

1. Un utente o un'applicazione richiede la risoluzione di un nome di dominio, come www.example.com.
2. Il client DNS locale effettua una query al proprio server DNS o al server DNS del provider Internet.
3. Se il server DNS locale non ha la risposta nella sua cache, invia una query a un server radice DNS.
4. Il server radice DNS fornisce l'indirizzo IP dei server DNS autorizzati per il dominio di primo livello (TLD) (ad esempio, .com).
5. Il server DNS locale quindi interroga il server DNS del TLD, che fornisce l'indirizzo IP dei server DNS autorizzati per il dominio di secondo livello (ad esempio, example.com).
6. Il server DNS locale effettua una query ai server DNS autorizzati per il dominio di secondo livello per ottenere l'indirizzo IP del nome di dominio specificato (www.example.com).
7. L'indirizzo IP viene restituito al client DNS locale, che lo memorizza nella sua cache per le future richieste.

Risoluzione inversa del DNS:

La risoluzione inversa del DNS è il processo di ottenere un nome di dominio da un indirizzo IP. Viene spesso utilizzata per tracciare indirizzi IP o scoprire i nomi di dominio associati a server o servizi.

Per eseguire una risoluzione inversa del DNS, si utilizza un record PTR (Pointer) nel database DNS. Un record PTR associa un indirizzo IP a un nome di dominio. Per esempio, un record PTR potrebbe associare l'indirizzo IP 192.0.2.1 al nome di dominio "mail.example.com". La risoluzione inversa è utile in scenari di sicurezza, monitoraggio di rete e gestione di server.