E’ come se fosse l’elenco telefonico di Internet.

Per accedere ad un sito internet, bisogna collegarsi ad un sito server ed ogni server è identificato da un numero chiamato indirizzo IP

www.pippocappuccio.it → ||| -- °°° → 123.45.67.89

Ricordare un indirizzo IP è molto complicato ed è per questo che si utilizzano degli indirizzi virtuali chiamati Hostname

Il compito del DNS è proprio questo

TRADURRE UN HOSTNAME IN INDIRIZZO IP

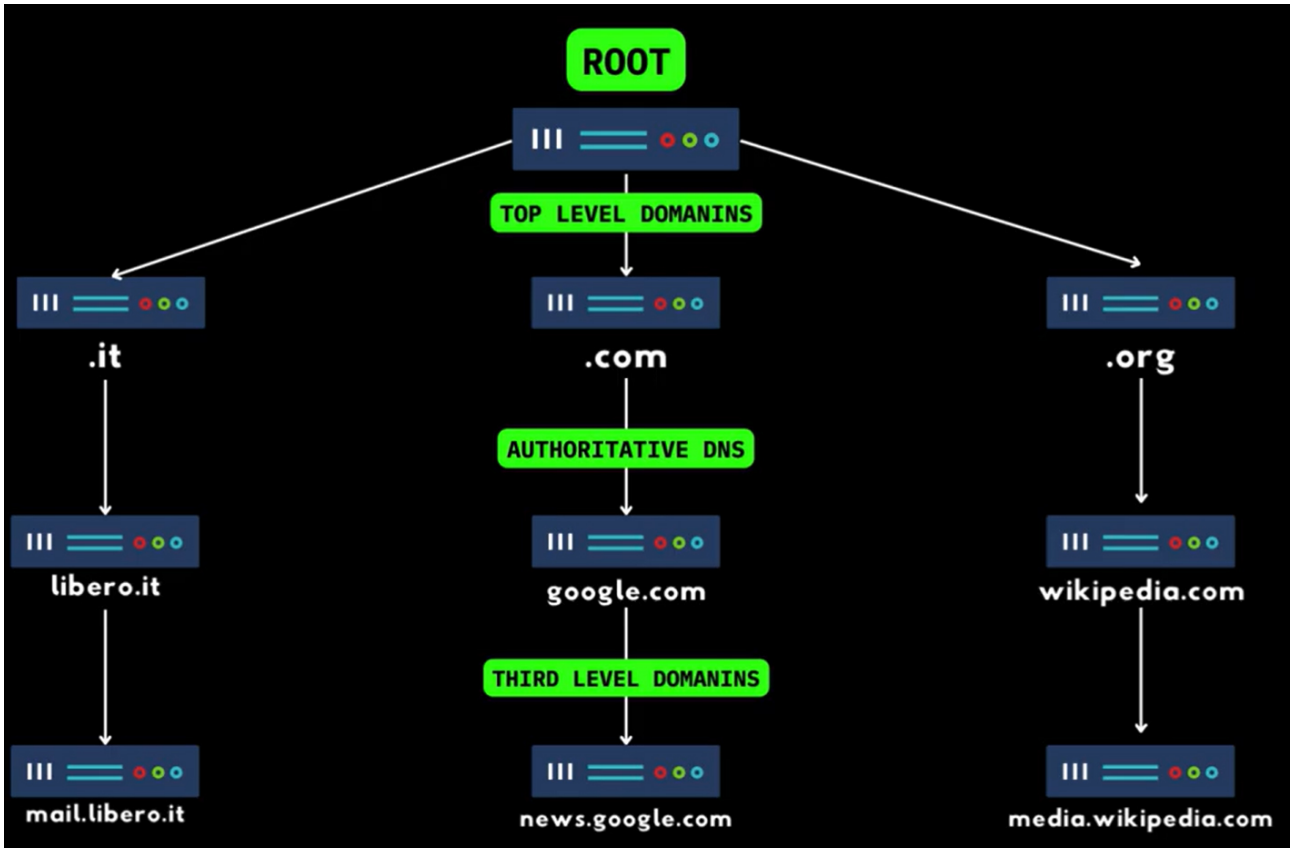
www.pippocappuccio.it 123.45.67.89

HOSTNAME INDIRIZZO IP

COME FA A FARLO ?

Immaginiamo il DNS come una grande biblioteca

gestita in maniera estremamente efficiente, al vertice di questa struttura c'è il bibliotecario capo, che rappresenta il server DNS ROOT ed



ovviamente questo bibliotecario non conosce tutti i libri, siti web nella biblioteca, ma sa esattamente a quali reparti, TOP LEVEL DOMAINS (TLD) indirizzarli. In ogni reparto c'è poi un bibliotecario, per esempio, c'è un bibliotecario per .it, uno per .com, uno per .org e così via. Questi bibliotecari, sanno quali scaffali, AUTHORITATIVE DNS, contengono le informazioni che stiamo cercando; infine ci sono i responsabili dei singoli scaffali, THIRD LEVEL.

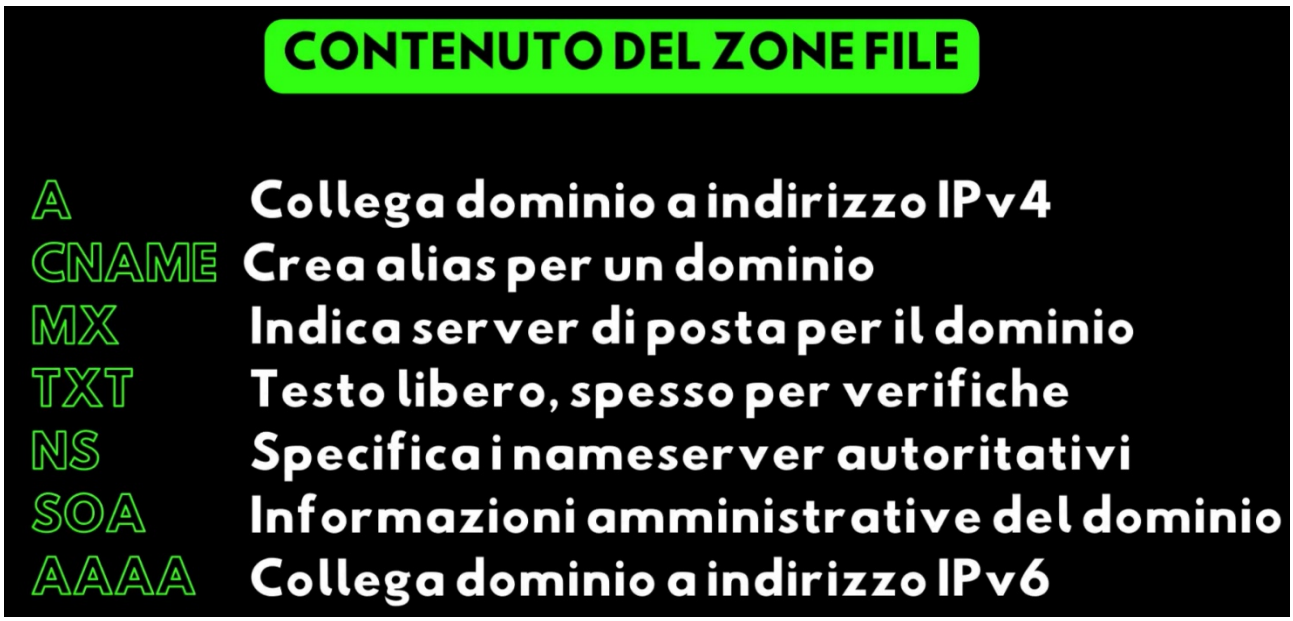
Il DNS può essere considerato come un enorme database distribuito, in grado di fornire la risposta in pochi ms (millisecondi). Per compare un dominio per un sito web ci si deve rivolgere ad un DOMAIN REGISTRAR, ovvero ad un'azienda che sia stata accreditata alla vendita di domini da **ICANN**

(Internet Corporation for Assigned Names and Numbers), un ente no-profit di gestione pubblica internazionale, istituito il 18 settembre 1998 per proseguire i numerosi incarichi di gestione relativi alla rete Internet che in precedenza erano demandati ad altri organismi, che però non si occupa direttamente della vendita.

Per ottenere l'indirizzo IP che ci serve, in maniera ancora più veloce, le risposte che il DNS ci ha fornito in precedenza, vengono memorizzate in nella memoria cache del browser o del sistema operativo per un certo periodo di tempo per poter essere riutilizzate successivamente.

Una volta acquistato un dominio, si possono modificare le impostazioni DNS ad esso associate utilizzando un file di configurazione, chiamato **ZONE FILE**

Nel Zone File è possibile



Il Domain Name System (DNS)

Obiettivi della lezione:

- Comprendere cos'è il DNS e perché è fondamentale per il funzionamento di Internet.
- Capire come funziona il processo di risoluzione dei nomi di dominio.
- Analizzare le componenti principali del DNS e i vari tipi di record DNS.
- Esplorare alcune vulnerabilità e attacchi comuni legati al DNS.

1. Introduzione al DNS

Il Domain Name System (DNS) è un sistema che traduce i nomi di dominio (come *www.esempio.com*) in indirizzi IP (come *192.0.2.1*). Gli esseri umani trovano più semplice ricordare nomi di dominio piuttosto che sequenze numeriche, quindi il DNS permette di accedere ai siti web usando nomi comprensibili invece che numeri.

2. Come funziona il DNS?

Il processo di traduzione di un nome di dominio in un indirizzo IP si chiama "risoluzione dei nomi" e avviene in più passaggi:

- **Passo 1: La richiesta del client**
  Quando un utente digita un URL nel browser, il computer invia una richiesta a un server DNS locale, spesso gestito dal proprio ISP (Internet Service Provider).
- **Passo 2: Risoluzione ricorsiva**
  Se il server DNS locale non ha una copia cache dell'indirizzo IP associato al dominio richiesto, invia una richiesta a un altro server DNS, chiamato *server di root*. I server di root indirizzano il server DNS locale al server autoritativo per il dominio richiesto.
- **Passo 3: Server autoritativo**
  Il server DNS autoritativo contiene le informazioni definitive sul dominio richiesto e restituisce l'indirizzo IP corrispondente al server DNS locale, che lo memorizza in cache per velocizzare richieste future.
- **Passo 4: Risposta al client**
  Il server DNS locale invia l'indirizzo IP al computer dell'utente, che può finalmente connettersi al sito web.

3. Componenti del DNS

Server di root: La parte iniziale della ricerca DNS. Ce ne sono 13 in tutto il mondo (di cui 10 presenti negli USA, due in Europa (Inghilterra e Svezia) ed uno in Giappone) e indirizzano le richieste verso i server appropriati (che sono indicati rispettivamente con le lettere dall'A alla M. Tutti dispongono di un indirizzo IPv4 e la maggior parte hanno anche un indirizzo IPv6. L'amministrazione dei root server rientra tra i compiti dell'ICANN (Internet Corporation for Assigned Names and Numbers), ma l'esecuzione è a cura di diverse istituzioni che garantiscono uno scambio dei dati nella zona di root sempre corretto, raggiungibile e sicuro. Questa panoramica mostra insieme ai gestori dei singoli root name server anche il loro indirizzo IP)

Lettera del DNS root server	Indirizzo IPv4	Indirizzo IPv6	Gestore
A	198.41.0.4	2001:503:ba3e::2:30	VeriSign
B	192.228.79.201	2001:478:65::53	USC-ISI
C	192.33.4.12	2001:500:2::c	Cogent Communications
D	199.7.91.13	2001:500:2d::d	University of Maryland
E	192.203.230.10		NASA
F	192.5.5.241	2001:500:2f::f	ISC
G	192.112.36.4		U.S. DoD NIC
H	128.63.2.53	2001:500:1::803f:235	US Army Research Lab
I	192.36.148.17	2001:7FE::53	Autonomica
J	192.58.128.30	2001:503:c27::2:30	VeriSign
K	193.0.14.129	2001:7fd::1	RIPE NCC
L	199.7.83.42	2001:500:3::42	ICANN
M	202.12.27.33	2001:dc3::35	WIDE Project

- **Server TLD (Top-Level Domain):** Gestiscono le richieste per domini di primo livello come *.com*, *.org*, *.it*.
- **Server DNS autoritativo:** Contiene le informazioni specifiche sui domini.

4. Tipi di record DNS

Ogni dominio può avere diversi tipi di record DNS, ognuno con uno scopo specifico:

- **A Record:** Associa un nome di dominio a un indirizzo IPv4.
- **AAAA Record:** Associa un nome di dominio a un indirizzo IPv6.
- **CNAME Record:** Fa riferimento a un altro nome di dominio, utile per creare alias (ad es., *www* può puntare a *esempio.com*).
- **MX Record:** Specifica i server di posta per un dominio.
- **TXT Record:** Memorizza informazioni testuali usate per varie verifiche e configurazioni (ad esempio, SPF per l'autenticazione delle email).

5. Vulnerabilità e attacchi legati al DNS

Il DNS, essendo un servizio fondamentale, è spesso bersaglio di attacchi informatici:

- **DNS Spoofing/Cache Poisoning:** Un attaccante introduce informazioni false nella cache del server DNS, facendo sì che il traffico venga reindirizzato verso un sito malevolo.
- **DDoS (Distributed Denial of Service):** Un attacco che mira a sovraccaricare i server DNS con un elevato numero di richieste, causando interruzioni di servizio.

6. Conclusioni e importanza del DNS

Il DNS è fondamentale per il funzionamento di Internet e rappresenta un'infrastruttura critica per garantire che gli utenti possano accedere ai servizi web in modo rapido e sicuro. È importante

comprendere come funziona e quali sono le sue vulnerabilità per saper gestire e proteggere le reti informatiche.

Compiti assegnati

1. Spiega in poche righe cos'è il DNS e a cosa serve.
2. Elenca i principali tipi di record DNS e descrivine uno.
3. Quali sono i principali rischi legati al DNS e come è possibile prevenirli?

Ecco le risposte ai compiti assegnati:

1. **Spiega in poche righe cos'è il DNS e a cosa serve.**
   Il DNS (Domain Name System) è un sistema che traduce i nomi di dominio (es. *www.esempio.com*) in indirizzi IP (es. *192.0.2.1*), permettendo agli utenti di accedere ai siti web utilizzando nomi facilmente memorizzabili invece di sequenze numeriche.
2. **Elenca i principali tipi di record DNS e descrivine uno.**
   - **A Record**: Associa un nome di dominio a un indirizzo IPv4.
   - **AAAA Record**: Associa un nome di dominio a un indirizzo IPv6.
   - **CNAME Record**: Crea un alias che punta a un altro nome di dominio.
   - **MX Record**: Specifica i server di posta per un dominio.
   - **TXT Record**: Contiene informazioni testuali usate per varie configurazioni e verifiche.

   Ad esempio, l'**A Record** associa un nome di dominio a un indirizzo IPv4 specifico, indicando al browser a quale indirizzo IP connettersi per visualizzare un sito web.

3. **Quali sono i principali rischi legati al DNS e come è possibile prevenirli?**
   - **DNS Spoofing/Cache Poisoning**: Un attacco in cui un hacker inserisce informazioni false nella cache del server DNS per reindirizzare il traffico a siti malevoli. Per prevenirlo, è possibile usare DNSSEC (Domain Name System Security Extensions), che garantisce l'integrità dei dati DNS.
   - **DDoS (Distributed Denial of Service)**: Un attacco che sovraccarica i server DNS con un numero enorme di richieste, rendendoli non disponibili. Per prevenirlo, si usano tecnologie come il rate limiting e infrastrutture ridondate per distribuire il carico.

Che cos’è il DNS?

Il DNS, o sistema dei **nomi di dominio**, è utilizzato per tradurre i nomi di dominio in indirizzi IP, consentendo ai browser di accedere ad altre risorse internet.

Quando gli utenti inseriscono un nome di dominio nella barra degli indirizzi del loro browser web, vengono portati al sito che vogliono visitare. Tuttavia, questo compito apparentemente im

mediato è costituito da diverse fasi, note come DNS lookup o processo di risoluzione DNS.

Ecco un esempio del processo di risoluzione DNS per illustrare meglio il funzionamento del DNS.

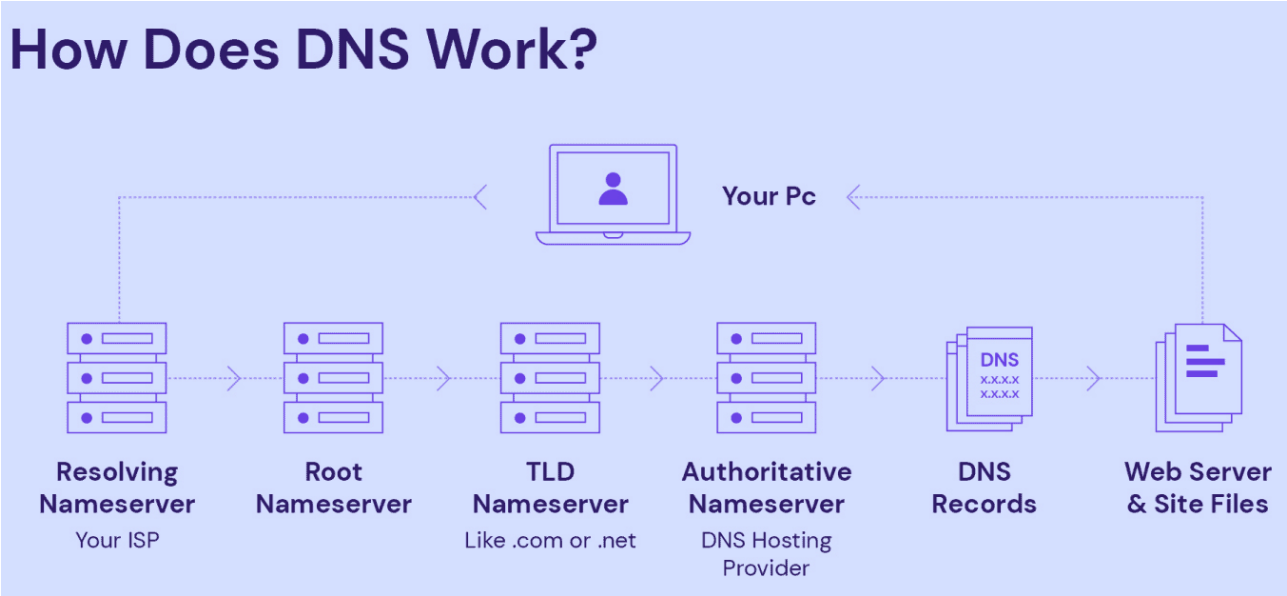
Vuoi essere indirizzato al sito web pippocappuccio.it, quindi inserisci il nome di dominio **piccocappuccio.it** nella barra degli indirizzi del browser web. In questo modo si invia una richiesta DNS.

Successivamente, il computer verificherà se ha già memorizzato una voce DNS del dominio inviato a livello locale. Un record DNS è un indirizzo IP che corrisponde al nome di dominio completamente qualificato.

Per prima cosa, il computer cercherà nel suo file hosts e nella sua cache. Il **file hosts** è un file di testo semplice che mappa i nomi host agli indirizzi IP in un sistema operativo, mentre la **cache** è un dato temporaneo memorizzato da un componente hardware o software.

Gli indirizzi IP corrispondenti al servizio DNS si trovano solitamente nella cache del browser o del provider di servizi internet (ISP).

Tuttavia, se nel file hosts e nella cache non si trova un indirizzo IP corrispondente, al processo di risoluzione DNS si aggiungono altri passaggi.



Quali server DNS sono coinvolti nel caricamento di un sito web?

Se il computer non trova un indirizzo IP corrispondente nel file hosts o nella cache, invia la query o la richiesta DNS a una rete di quattro

server DNS. La sezione seguente illustra i singoli server DNS e il loro funzionamento.

Resolver DNS

Il **resolver DNS** o resolver ricorsivo funge da intermediario principale tra un computer e gli altri server DNS. Il suo scopo è quello di inoltrare una richiesta ad altri server del sistema dei nomi di dominio per poi rispedirla indietro una volta soddisfatta.
Quando il resolver DNS riceve una richiesta, per prima cosa cerca nella sua cache un indirizzo IP corrispondente al nome di dominio. Se tale indirizzo IP viene trovato, la richiesta inviata ai server DNS termina qui e l'utente vedrà immediatamente il sito che desidera visitare.
Tuttavia, se non viene trovata alcuna corrispondenza nella sua cache, il resolver DNS invierà la richiesta al server DNS successivo: il root nameserver.

Root nameserver

Il **root nameserver** o **server root DNS** si trova in cima alla gerarchia DNS. Consideralo come una banca di riferimento.
Non conserva l'informazione che si sta cercando, ovvero l'indirizzo IP che corrisponde al nome di dominio, ma fornisce indicazioni su dove è possibile trovarlo.
Quando il root nameserver riceve una richiesta dal resolver DNS ricorsivo, identifica il **dominio di primo livello** del nome di dominio. Quindi, indicherà al resolver ricorsivo di andare al nameserver TLD corretto.

Nameserver TLD

Il **nameserver TLD** è una funzione del server DNS responsabile della memorizzazione e della gestione delle informazioni sui nomi che

utilizzano uno specifico **dominio di primo livello (TLD)**. Un TLD è l'estremo di un nome di dominio, come **.it**, **.com**, **.org**, **.online** e **.net**. Se la richiesta è di trovare l'indirizzo IP di pippocappuccio.it, il root nameserver reindirizzerà il resolver DNS ricorsivo al nameserver TLD **.it**. Successivamente, il nameserver TLD informerà il resolver sulla posizione dell'indirizzo IP corrispondente presso uno specifico namerserver autoritativo.

Nameserver autoritativo

Il **nameserver autoritativo** o **server DNS autoritativo** è l'autorità finale nel processo di risoluzione DNS. Memorizza tutte le informazioni relative al nome di dominio che si desidera visitare, compreso il suo indirizzo IP. Il resolver ricorsivo ottiene l'indirizzo IP e lo rimanda al tuo computer, indirizzandoti al sito.
Infine, il resolver del sistema dei nomi di dominio esegue il **caching DNS**, memorizzando gli indirizzi IP raccolti dai nameserver autoritari come dati temporanei. In altre parole, la memorizzazione nella cache DNS fa sì che la volta successiva che si desidera visitare lo stesso sito, il risolutore rimandi semplicemente l'indirizzo IP ottenuto in precedenza.