DNS

Domain Name System

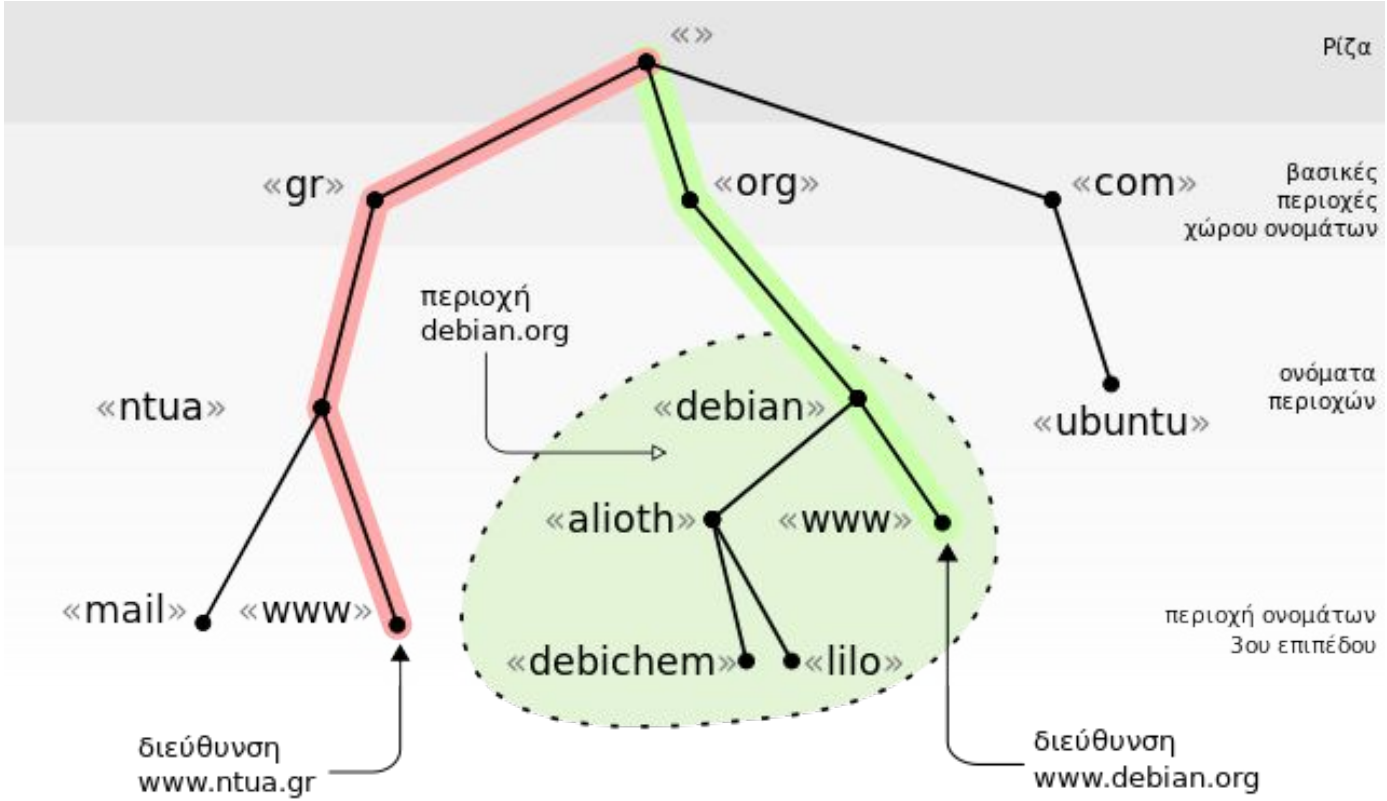
Domain Name System

È un sistema articolato che ha il compito di mappare i nomi dei nodi nei loro indirizzi IP.

La struttura del DNS ha una gestione che consente in modo semplice di evitare conflitti nei nomi e che è efficiente, ottenendo buone performance usando poche risorse.

Non viene utilizzato un repository centrale, ma una directory distribuita, basata su uno spazio dei nomi gerarchico e un protocollo automatizzato.

Il processo di “traduzione” di un nome nel corrispondente indirizzo prende il nome di “risoluzione” del nome.



DNS_Tree.svg: Sylvain Leroux (talk)derivative work: Ggia, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

DNS: lo spazio dei nomi

Lo spazio dei nomi è rappresentato da un albero, ogni sottoalbero è un dominio. I nomi si compongono dalla foglia alla radice.

Ad esempio,

robot.cs.washington.edu

è la risorsa robot nel dominio cs.washington.edu, sottodominio di washington.edu, sottodominio di edu, sottodominio della radice ".", che normalmente viene omessa.

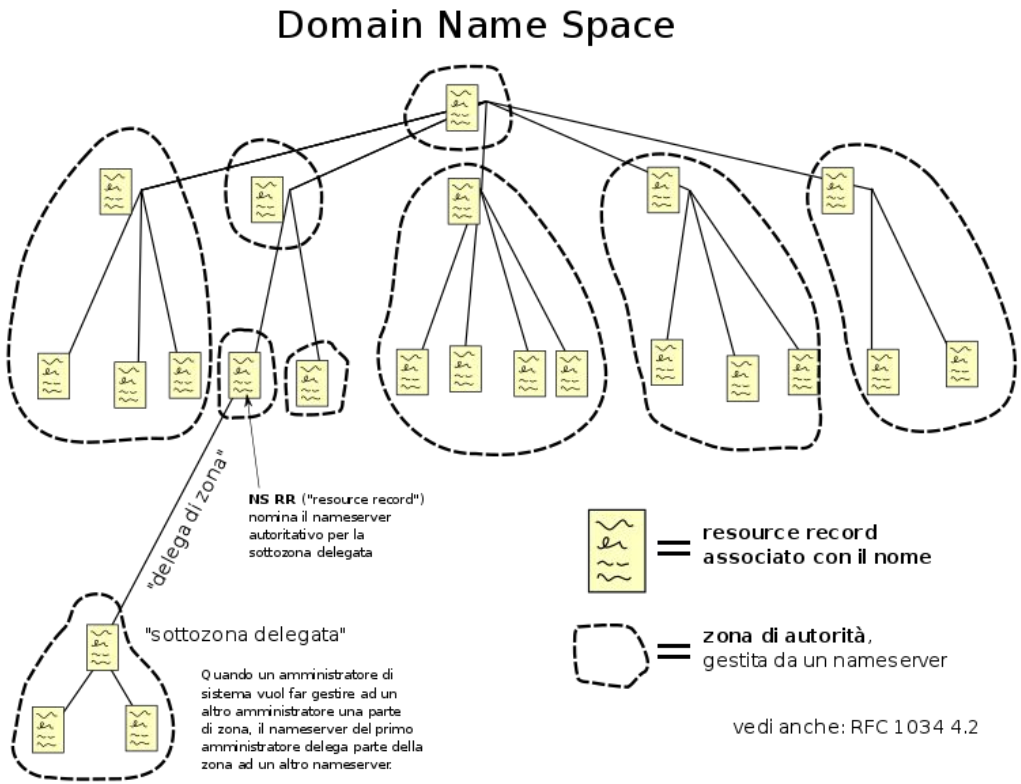
DNS: lo spazio dei nomi

I nomi di primo livello (TLD) sono gestiti da ICANN Internet Corporation for Assigned Names and Numbers).

I TLD generici (es., .edu, .com, .net,...) descrivono intere categorie, ma sono utilizzati prevalentemente negli USA.

I country code TLD (es., .it,.uk, .es) derivano da una lista standard di nazioni e sono pensati per un utilizzo nazionale.

Alcuni di essi (come ad es. .tv, delle Isole Tuvalu o .fm, Federated Islands of Micronesia) sono commercializzati all'esterno.



Di Lion Kimbro (original author); Mess (derivative work) – File:Domain name space.svg, CCo, https://commons.wikimedia.org/w/index.php?curid=75965575

Spazio dei nomi

Lo spazio dei nomi è diviso in zone, che sono alla base della distribuzione.

Una zona è una porzione delle spazio dei nomi servita da un server DNS che è il server autorevole di quella zona.

Il server autorevole gestisce tutte le informazioni della zona, comprese le informazioni di delega che dicono quae server contattare per la risoluzione dei nomi di un sottodominio.

Mentre i domini si sovrappongono, le zone non si sovrappongono.

Resource Records

Host (A) record

Definisce la corrispondenza tra un nome di dominio e un indirizzo IPv4

A6 record

Definisce la corrispondenza tra un nome di dominio e un indirizzo IPv6

Pointer (PTR) record

E’ utilizzato nella risoluzione inversa, associa a un indirizzo IP un nome di dominio

Resource Records

Alias (CNAME) record

Associa un nome di dominio ad un altro nome di dominio (es. dati.mydomain.com potrebbe puntare a server1.mydomain.com)

Mail Exchanger (MX) record

Specifica il server SMTP do posta elettronica di un dominio.

Nameserver (NS) record

E’ utilizzato per definire il nameserver autorevole di una zona

Resource Records

Start of Authority (SOA) record

Contiene tutte le informazioni sulla zona gestita dal name server autorevole.

Service (SRV) record

Specifica un servizio attivo in un determinato dominio.

Text (TXT) record

Utilizzato per descrivere un dominio

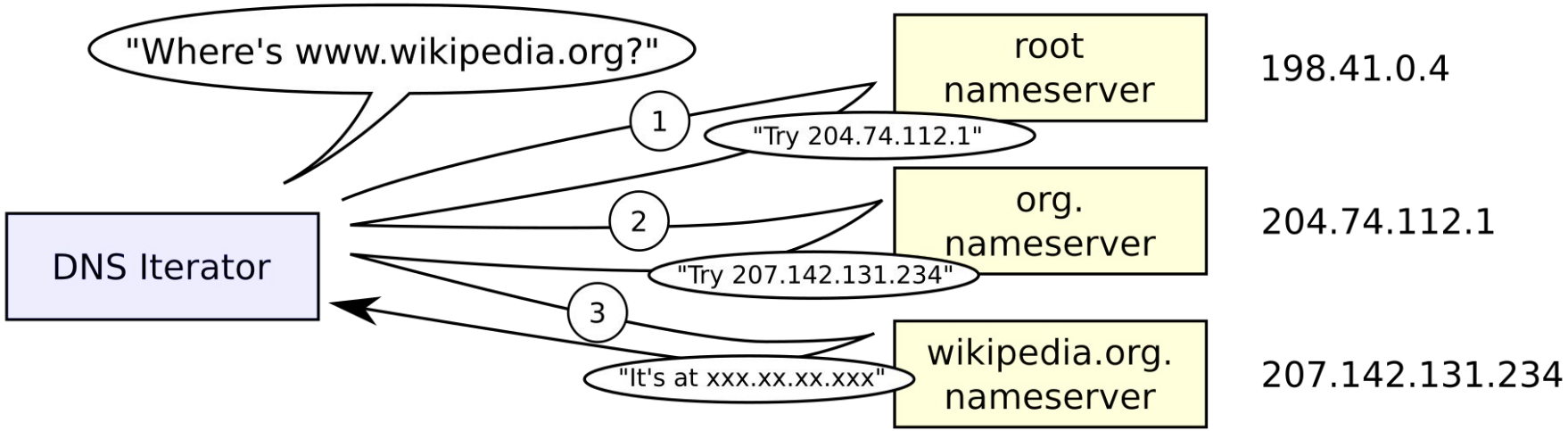
Configurazione name server

```
@             IN    NS   dns.itiseveri.org.
dns           IN    A    10.0.2.254
www           IN    A    10.0.2.1
labinfo       IN    NS   dns.labinfo.itiseveri.org.
dns.labinfo   IN    A    10.0.1.254
```

Il nameserver di itiseveri.org delega il nodo 10.0.1.254 a gestire il sottodominio

```
@     IN    NS   dns.labinfo.itiseveri.org.
dns   IN    A    10.0.1.254
pc1   IN    A    10.0.1.1
```

La configurazione del nameserver delegato



Risoluzione dei nomi: procedimento iterativo

La risoluzione dei nomi avviene con un procedimento iterativo che parte con una richiesta al root name server.

Il root name server risponde con le indicazioni necessarie a contattare il name server autorevole del TLD, e così via a scendere nella gerarchia fino a raggiungere (con query successive) il name server autorevole che gestisce il record relativo al nome richiesto, e che quindi può fornire l'indirizzo IP cercato.

In questo modo viene semplificato il compito dei name server autorevoli.

Risoluzione dei nomi: procedimento ricorsivo

Normalmente i client DNS si rivolgono a un name server locale (che tipicamente risiede nel router).

Il name server locali avviano la risoluzione iterativa seguendo la gerarchia dei name server autorevoli e restituiscono ai client direttamente la risposta. Questo procedimento prende il nome di risoluzione ricorsiva.

I name server locali memorizzano nella propria cache sia i risultati finali della risoluzione iterativa che tutti i risultati intermedi (nomi ed indirizzi dei name server autorevoli contattati), velocizzando quindi le successive richieste di risoluzione.

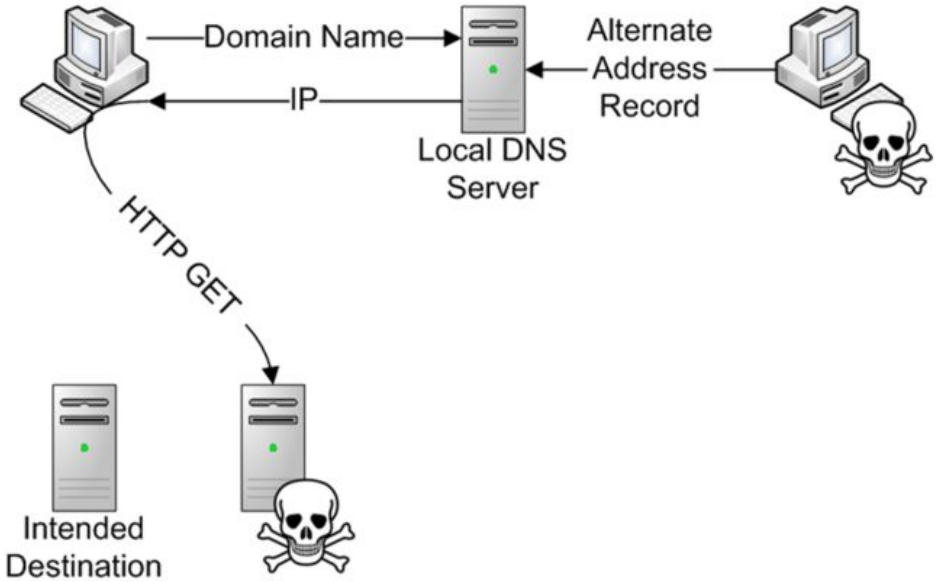
Protocollo DNS

Il protocollo DNS è un semplice protocollo domanda-risposta che lavora su UDP. I server sono in ascolto sulla porta 53.

Il client invia una query, ogni query ha un proprio identificativo a 16 bit. Il server risponde e la risposta riporta lo stesso identificativo. In questo modo, è possibile "collegare" la risposta alla domanda.

Se il client non riceve la risposta in un tempo ragionevole (il protocollo UDP non è affidabile), la reinvia (Automatic Repeat reQuest).

DNS Cache Poisoning



DNS spoofing

Un attacco DNS spoofing ha lo scopo di inserire nella cache di un name server locale la risoluzione fraudolenta di un nome di dominio.

- l'attaccante invia al name server locale la richiesta di risoluzione del nome da falsificare;
- il server locale inizia il procedimento di risoluzione iterativo verso i name server autorevoli, contemporaneamente l'attaccante inizia ad inviare delle risposte fasulle con spoofing dell'indirizzo IP del server autorevole e identificativo variabile;
- se una delle risposte dell'attaccante "indovina" l'identificativo della query, questa viene considerata valida e memorizzata nella cache.

DNSSEC

È un’estensione del protocollo DNS che consente di validare le risposte dei name server.

Ogni name server autorevole ha un certificato con cui “firma” le risposte che invia. Quando la risposta serve ad identificare il name server autorevole di un sottodominio, la risposta contiene anche il certificato di tale server.

In questo modo i name server locali devono conoscere solo il certificato del root name server.