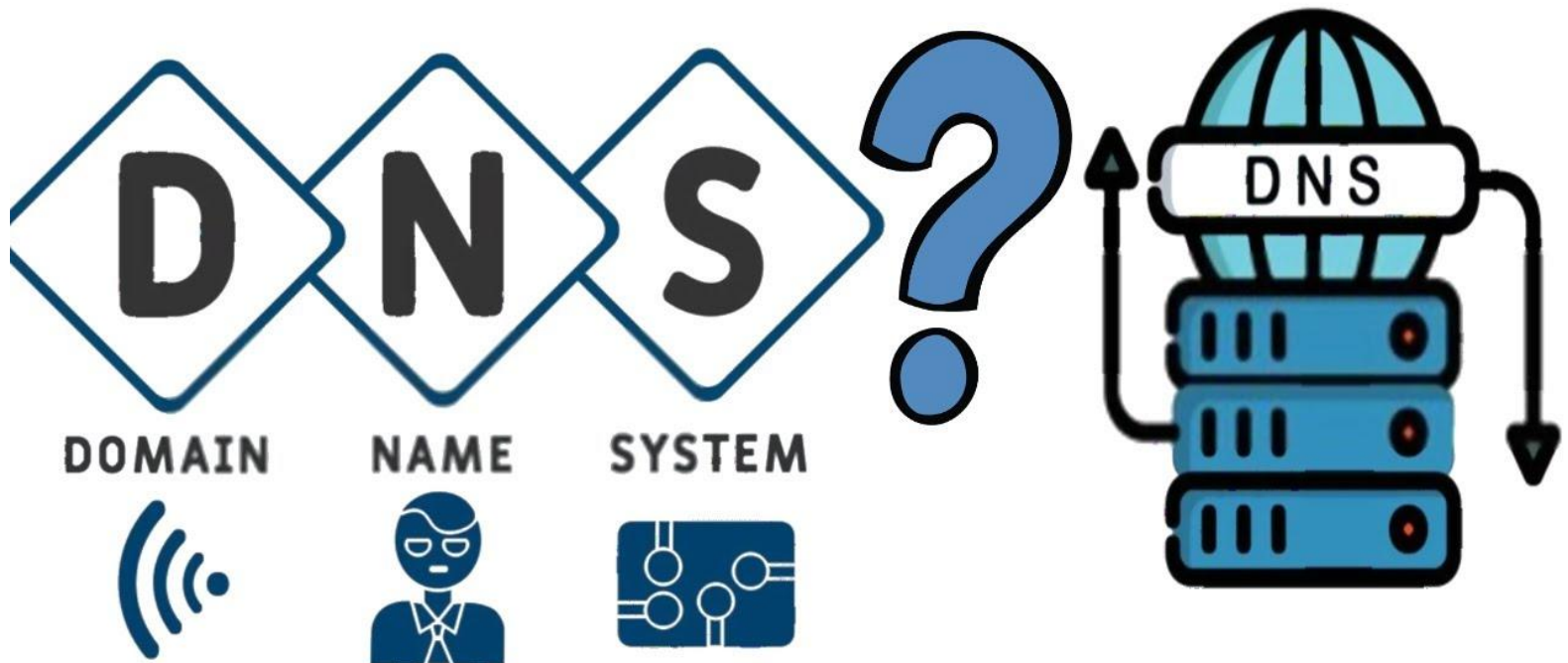
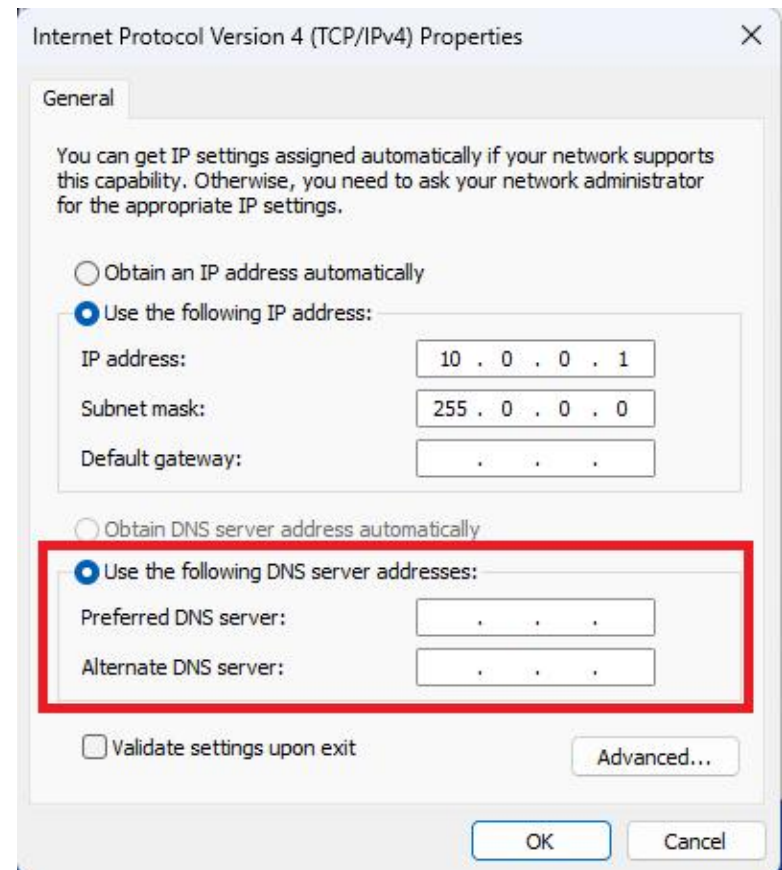


Dịch vụ DNS (Domain Name System)

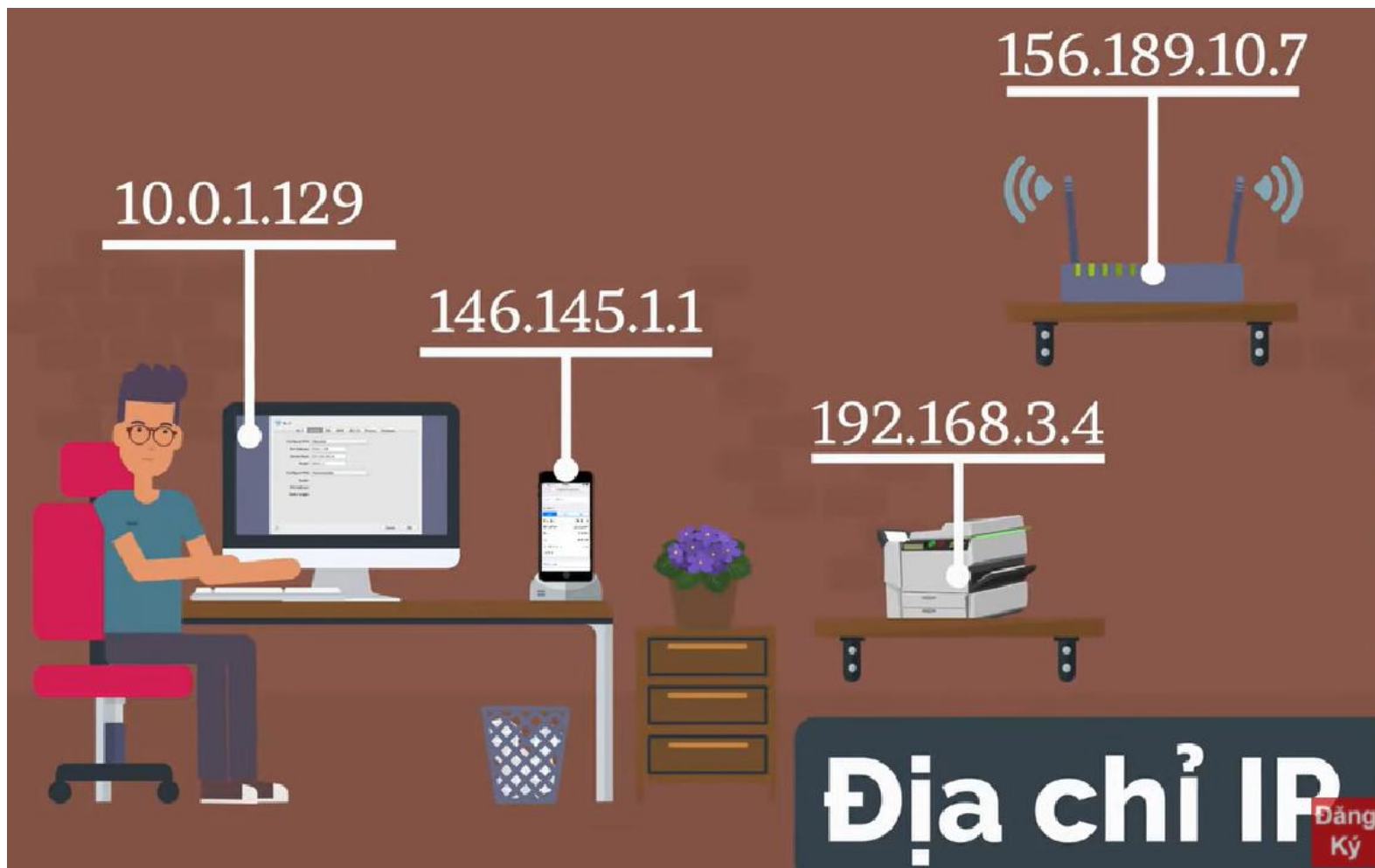


Tự tìm hiểu

- DNS dùng để làm gì?
- Có mấy loại DNS Server? Kể tên.

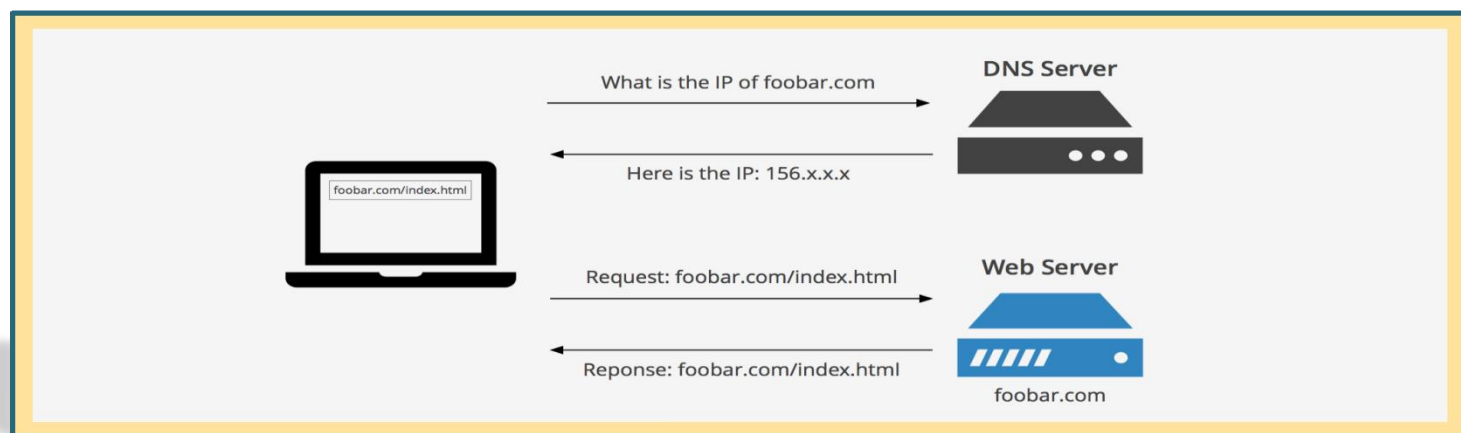


TỔNG QUAN



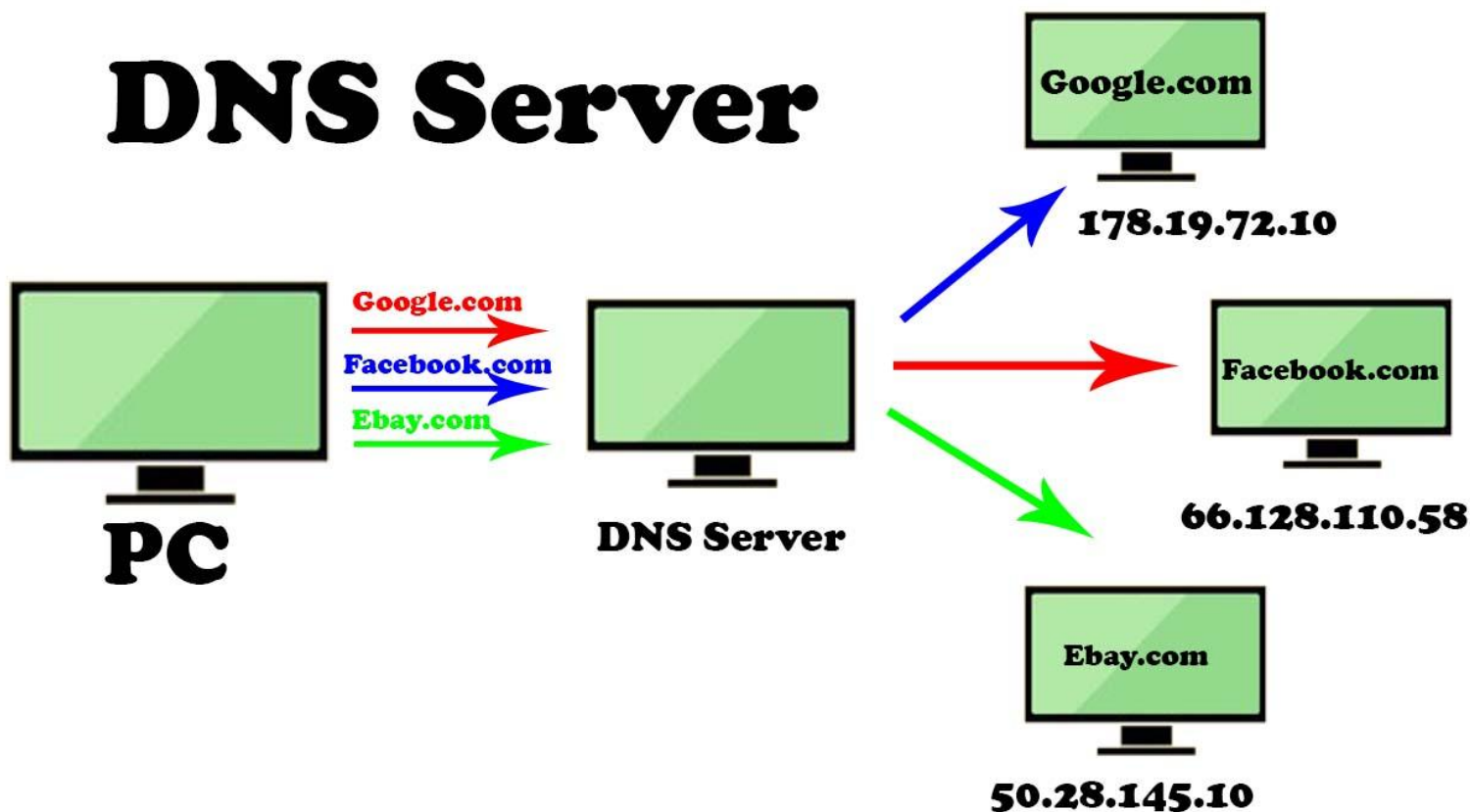
Địa chỉ IP Đăng Ký

- Hệ thống phân giải tên miền (hay được viết tắt là **DNS** . Tên tiếng Anh ***Domain Name System***) là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet và ngược lại



Ví dụ:

DNS Server



Tên miền và Top-Level Domain

Domain: Một nhánh các bản ghi trong CSDL DNS. Một domain có thể chia thành các domain con (subdomain).

Domain Name: Mỗi domain có một domain name chỉ vị trí của nó trong CSDL. Một tên miền là các nhãn ghép với nhau phân cách bởi dấu chấm (.).

Top-Level Domain: Là nhãn phía phải nhất trong tên miền. Sau nó là Second-Level Domain.





www.example.com
subdomain second-level domain TLD

Cấu trúc tên miền

Một số Top Level Domain thường thấy:

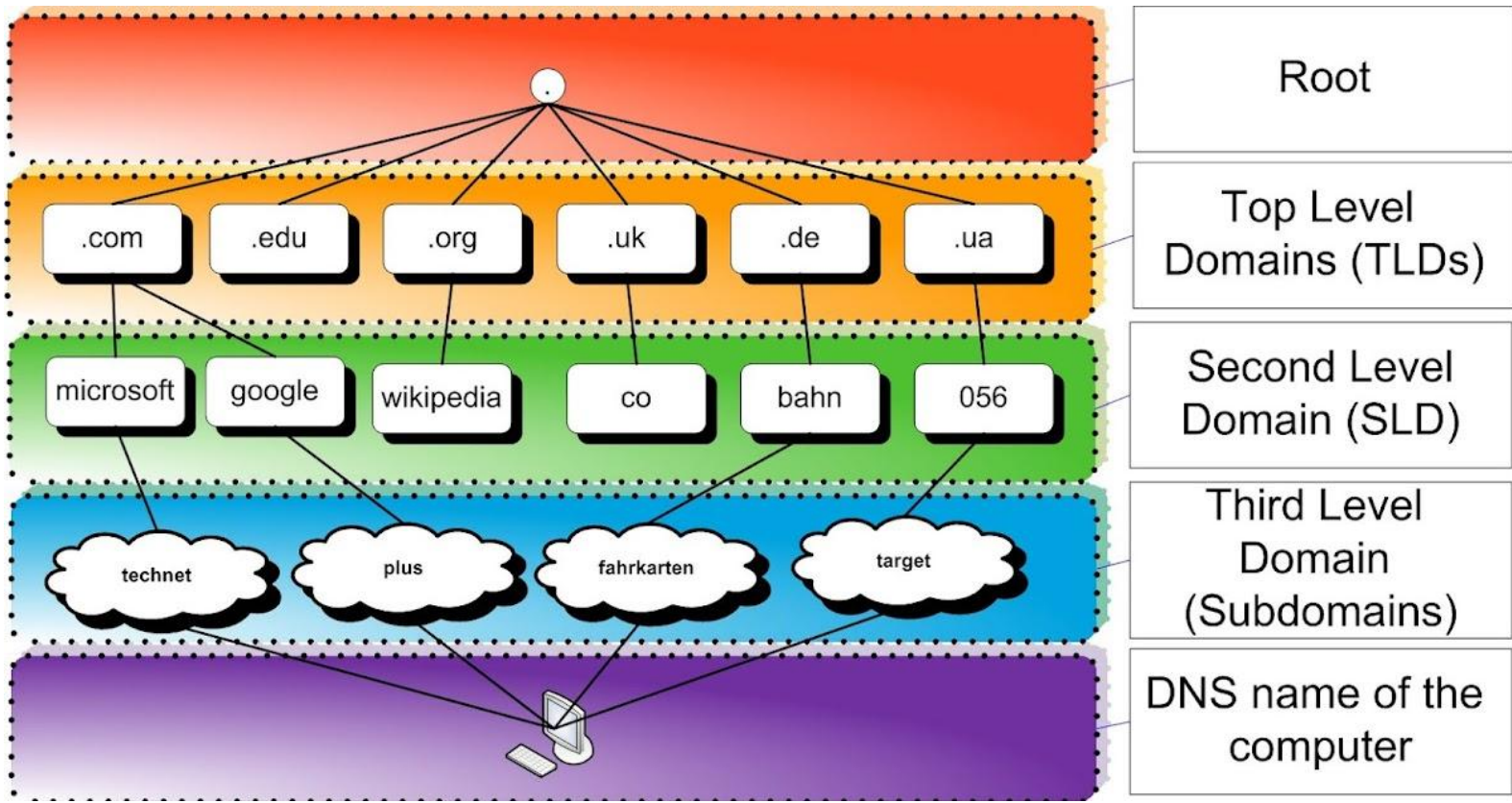
Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ

Top Level Domain theo quốc gia được ưu tiên hơn:

Tên miền	Mô tả
.vn	Việt Nam
.us	Mỹ
.jp	Nhật bản
.cn	Trung quốc

Vd: hau1.edu.vn
.vn là Top Level Domain





Các loại DNS Server

- Recursive resolver
- Root nameserver
- TLD nameserver
- Authoritative nameserver



Recursive resolver

- Điểm dừng đầu tiên trong quá trình truy vấn DNS. Nó hoạt động như một cầu nối trung gian giữa máy client và DNS nameserver
- Sau khi nhận được truy vấn DNS từ một client web thì recursive resolver sẽ phản hồi với dữ liệu được lưu trong bộ nhớ cache hoặc gửi yêu cầu đến root nameservers tiếp theo là đến TLD nameservers và cuối cùng đến authoritative nameserver.



Recursive resolver

- Sau khi nhận được phản hồi từ authoritative nameserver chứa địa chỉ IP được yêu cầu, recursive resolver sẽ gửi phản hồi cho Client.
- Recursive resolver sẽ lưu trữ thông tin nhận được từ authoritative nameserver. Khi một Client yêu cầu địa chỉ IP của một tên miền giống với client trước yêu cầu thì recursive resolver sẽ cung cấp các bản ghi được yêu cầu từ bộ nhớ cache của nó. Bỏ qua quá trình hỏi root nameservers.



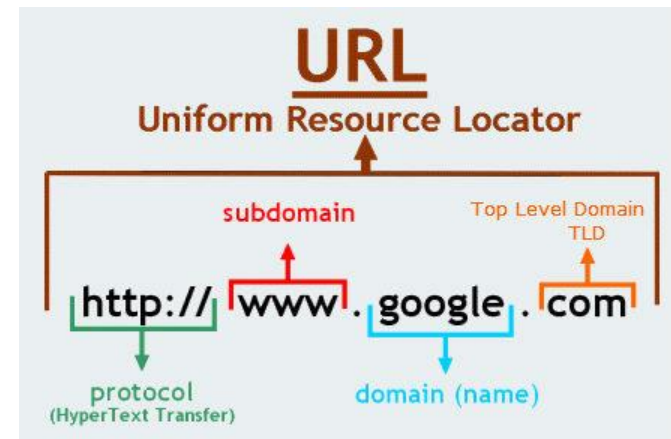
Root Name Server

- Quá trình tìm kiếm tên miền luôn được bắt đầu bằng các truy vấn gửi cho máy chủ ROOT.
- Root nameservers chấp nhận truy vấn của recursive resolver gồm một tên miền và thực hiện trả lời bằng cách hướng recursive resolver đến TLD nameservers dựa trên phần mở rộng của tên miền đó (.com, .vn, .net, .org,...). Các Root nameservers này được giám sát và theo dõi bởi Internet Corporation for Assigned Names and Numbers (ICANN).
- Trên mạng Internet hiện tại có tất cả 13 hệ thống máy chủ tên miền ở mức ROOT.



TLD Nameserver

Top-level Domain là phần mở rộng của tên miền. Nó là những chữ đi sau dấu chấm cuối cùng của một tên miền. Ví dụ, trong www.google.com thì TLD là com. Và Server cho TLD gọi là TLD Nameserver. Công việc của nó quản lý toàn bộ thông tin phần mở rộng của tên miền.

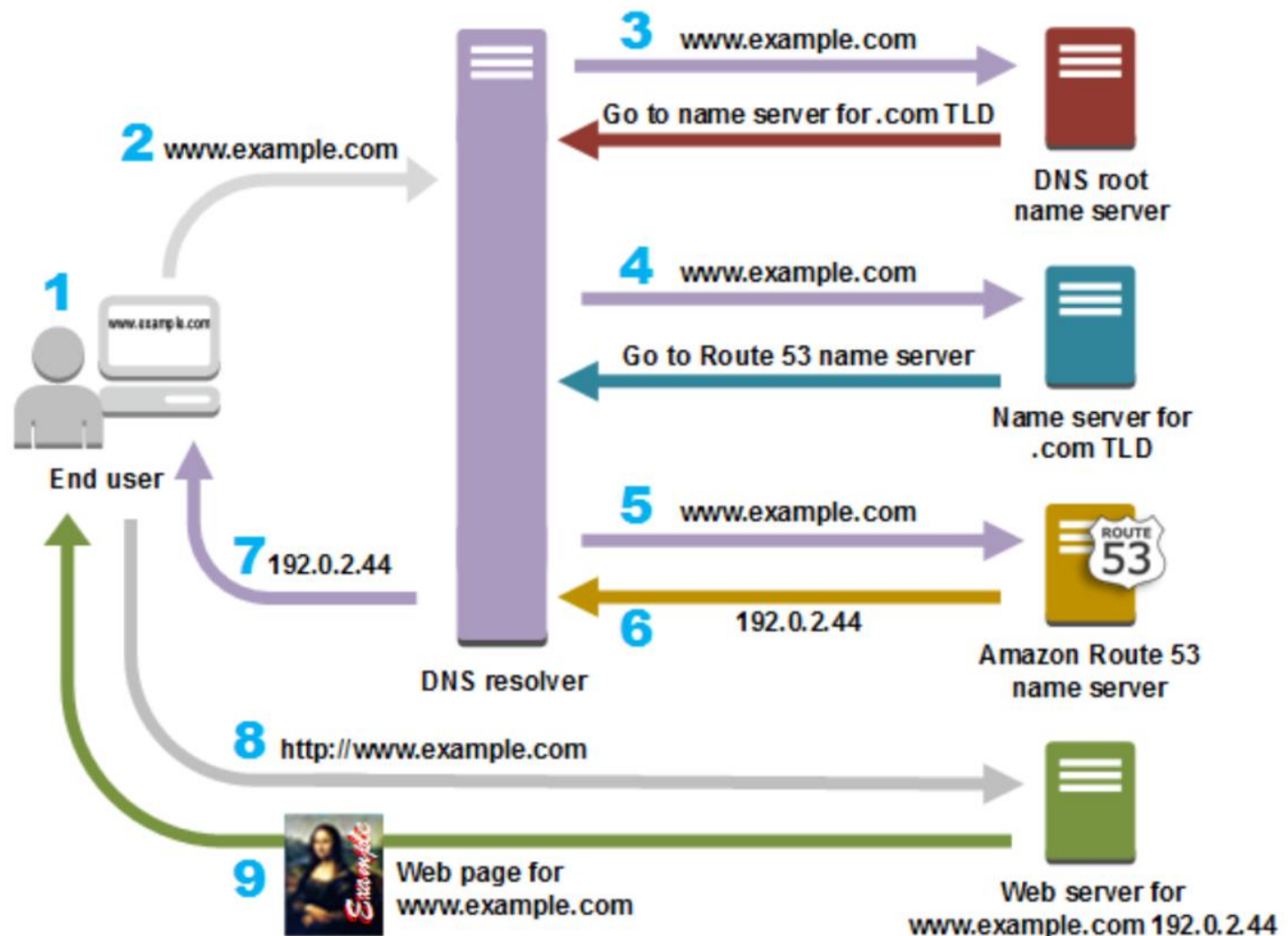


Authoritative Name Server

Khi recursive resolver nhận được phản hồi từ TLD nameservers, phản hồi đó sẽ hướng recursive resolver đến authoritative nameserver. Đây chính là bước cuối cùng mà recursive resolver sẽ tìm được tìm địa chỉ IP cần tìm kiếm.



Cơ chế hoạt động của DNS



Cài đặt DNS

- Cài đặt Name Server

```
$sudo apt install bind9
```

- Cài đặt các công cụ hỗ trợ

```
$sudo apt install bind9utils
```

```
$sudo apt install bind9 bind9utils
```



Cấu hình DNS

- Server DNS thường dùng trên Linux là server named. Các thông số cấu hình được qui định qua các file.

VD:

- Thiết lập DNS server phân giải miền thuchanh.net thành 192.168.14.10 và ngược lại.



nano /etc/bind/named.conf.options

#xác định danh sách các máy khách được phép các truy vấn DNS
options {

#qui định thư mục chứa các file cấu hình

directory “/var/cache/bind” ;

#khi nhận được 1 query không biết, gửi tiếp

#cho 1 DNS server khác để hỏi

forwarders { 192.168.14.10; };

};



nano /etc/bind/named.conf.local

create new

add zones for your network and domain name

```
zone "thuchanh.net" IN {  
    type master;  
    file "/etc/bind/db.thuchanh.net";  
};  
zone "14.168.192.in-addr.arpa" IN {  
    type master;  
    file "etc/bind/db.192;  
};
```




- *.*.*.*.in-addr.arpa

trường hợp 10.0.0.0/24

- network address \Rightarrow 10.0.0.0
- network range \Rightarrow 10.0.0.0 - 10.0.0.255
 \Rightarrow 0.0.10.in-addr.arpa
- # case of 192.168.14.10/24
- # network address \Rightarrow ?
- # network range \Rightarrow ?
 \Rightarrow ?.in-addr.arpa





Tạo 2 file CSDL DNS (db.thuchanh.net, db.192) bằng cách copy từ file mẫu db.local và db.127 (đỡ phải gõ)

- cp /etc/bind/db.local
/etc/bind/db.thuchanh.net
- cp /etc/bind/db.127 /etc/bind/db.192

nano /etc/bind/db.thuchanh.net

Tạo file zone: các server phân giải thành địa chỉ ip từ tên miền

\$TTL 604800

@ IN SOA thuchanh.net. root.thuchanh.net. (

2 ;Serial

3600 ;Refresh after 1 hour

1800 ;Retry after 30 minute

604800 ;Expire after 1 week

86400 ;Minimum TTL of 1 day

);

@ IN NS thuchanh.net. # define Name Server

@ IN A 192.168.14.10 # define Name Server's IP address

@ IN AAAA ::1

ns IN A 192.168.14.10



nano /etc/bind/db.192

Tạo file zone: các server phân giải thành tên miền từ địa chỉ ip
\$TTL 86400

```
@ IN SOA thuchanh.net. root.thuchanh.net. (  
    1 ;Serial  
    3600 ;Refresh  
    1800 ;Retry  
    604800 ;Expire  
    86400 ;Minimum TTL  
);
```

define Name Server

```
@ IN NS ns.  
10 IN PTR ns.thuchanh.net.
```



- Số serial: Luôn tăng số này lên 1 mỗi khi thay đổi dữ liệu trên primary server, các secondary sẽ so sánh con số này để biết dữ liệu của nó lưu trữ đã cũ hay chưa và có cần update mới hay không.
- Refresh: Chỉ ra khoảng thời gian máy chủ Secondary kiểm tra dữ liệu trên máy Primary để cập nhật.
- Retry: Nếu máy chủ secondary không kết nối được với máy chủ primary để update dữ liệu, nó sẽ cố gắng thử lại sau mỗi khoảng thời gian retry.
- Expire: Nếu sau khoảng thời gian expire này mà máy chủ secondary vẫn không liên lạc được với máy chủ primary thì nó xem thông tin nhận từ máy chủ primary từ trước đó là quá hạn.
- TTL: Chỉ ra khoảng thời gian mà các máy chủ khác được phép cache lại thông tin trả lời. Quá thời hạn này các máy chủ caching name server phải thực hiện lại việc truy vấn, không sử dụng lại các giá trị truy vấn đã lưu.



- SOA: Chỉ ra rằng máy chủ Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.
- NS: Mỗi name server cho zone sẽ có một NS record.
- A: Record A (Address) ánh xạ tên máy (hostname) vào địa chỉ IP.
- CNAME: Record CNAME (canonical name) tạo tên bí danh alias trỏ vào một tên canonical.
- PTR: Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành hostname.



Thay đổi DNS

```
# nano /etc/resolv.conf
```

```
nameserver 192.168.14.10
```

Khởi động lại BIND

```
# systemctl restart bind9
```



Dùng lệnh nslookup để kiểm tra



KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ HÀ NỘI