

**“DNS là gì?”** – Thật ra, trong thế giới công nghệ nói chung và thiết kế website nói riêng, kể cả đối với những người học không chuyên sâu về công nghệ thông tin đều đã từng nghe hoặc biết đến cụm từ viết tắt này rồi.

Song tôi cũng khá chắc chắn rằng khi bạn tìm thấy bài viết này, hoặc bạn đang bắt đầu tìm hiểu về khái niệm DNS từ con số 0, hoặc bạn đang “vật lộn” với hàng tá thông tin mơ hồ, “cao siêu” nhưng khó hiểu nhặt nhạnh từ nhiều nguồn khác nhau.

Nhưng đừng quá lo lắng, tôi và bạn sẽ cùng ngồi lại để chia sẻ với nhau “tất tần tật” những thông tin tổng hợp về DNS sau khi bạn mua tên miền cũng như những ảnh hưởng “siêu to khổng lồ” của hệ thống này đối với mạng Internet.

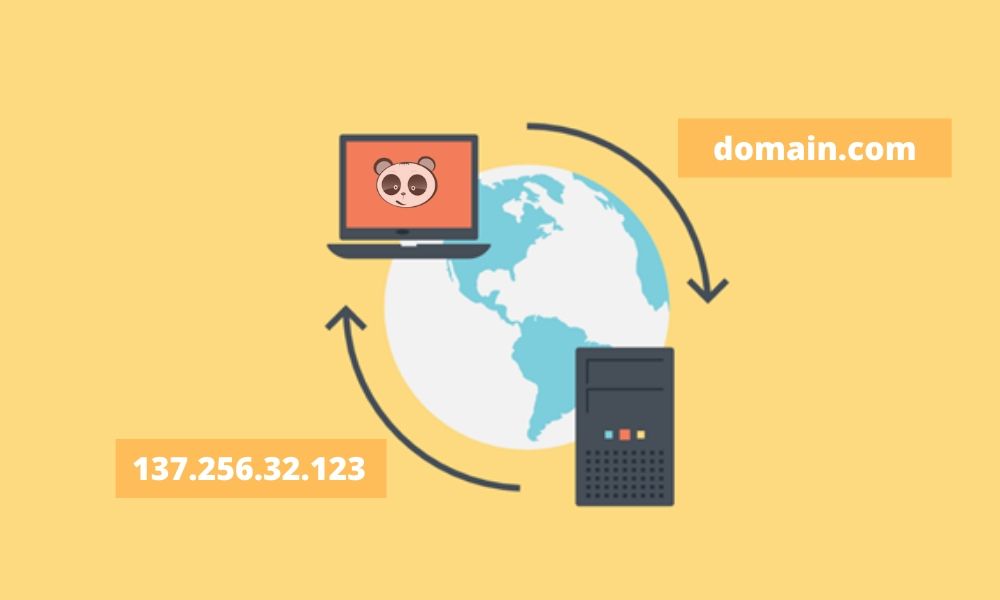
Chúng ta bắt đầu ngay nhé!.

1. **Khái niệm DNS**

DNS (Domain Name System) hay hệ thống phân giải tên miền, có thể được giải thích là một hệ thống giúp con người và máy tính có thể “giao tiếp” với nhau một cách dễ dàng hơn (Vì ngôn ngữ giao tiếp của chúng ta là tên và chữ viết, còn máy tính chỉ có thể hiểu được các dãy số mà thôi!) Hệ thống giúp biên dịch tên miền (hostname) thành các dãy số, để máy tính có thể hiểu được.

1. **Mục tiêu**

Nhìn chung, mục tiêu của DNS tương đối đơn giản, chỉ là giúp mọi người dễ nhớ hơn những chuỗi số dài, khó hiểu. Cơ mà vai trò của của nó lại rất quan trọng trong thời đại 4.0 – thời đại mà những kết nối ngày càng phát triển. Nó sẽ càng trở nên quan trọng hơn khí IPv6 (Giao thức liên mạng thế hệ 6) trở nên thịnh hành, thay thế IPv4 như 192.168.0.1 bằng một các gì đó như fdf8:82e4::53.



1. **Chức năng của DNS**

Domain name system cũng giống như một cuốn danh bạ điện thoại. Nghĩa là thay vì bạn phải nhớ hàng tá số điện thoại với một đống con số, thì bạn chỉ cần nhớ tên của chủ nhân số điện thoại thôi. Mà trong trường hợp, thì số điện thoại sẽ tương ứng với địa chỉ IP của Website, còn tên chủ nhân chính là tên miền của website đó.

Ví dụ, khi bạn gõ “www.google.com” vào trình duyệt, máy chủ DNS sẽ lấy địa chỉ của máy chủ Google là “74.125.236.37”. Sau đó, bạn sẽ thấy trang home của Google tải trang trên trình duyệt mà bạn đang sử dụng. Đó là quá trình phân giải DNS.

Ngoài ra thì mỗi DNS còn có chức năng ghi nhớ những tên miền mà nó đã phân giải và trong những lần truy cập tới, nó sẽ ưu tiên sử dụng. Đó là lý do mà bạn sử dụng nhiều dịch vụ mạng như research thông tin, xem phim, chơi game giải trí,… nhanh chóng và dễ dàng hơn.

1. **Cách hoạt động của DNS**

DNS hoạt động từng bước theo cấu trúc của nó. Bước đầu là một truy vấn để lấy thông tin được gọi là “DNS query” .

Lại quay về với ví dụ tìm kiếm website www.google.com trong web browser nhé!

→ Đầu tiên, DNS server sẽ tìm thông tin phân giải trong file hosts – tức file text trong hệ điều hành, chịu trách nhiệm chuyển hostname thành IP.

* Nếu không thấy thông tin, nó sẽ quay về tìm trong cache – bộ nhớ tạm của phần cứng hay phần mềm. Nơi phổ biến nhất thường lưu thông tin này chính là bộ nhớ tạm của trình duyệt và bộ nhớ tạm ISP (Internet Service Providers.
* Nếu không nhận được thông tin, bạn sẽ thấy mã bị lỗi hiện lên.

1. **Các loại DNS Server và vai trò**

Trên thực tế, có đến tổng cộng khoảng 4 server tham gia vào trong hệ thống phân giải tên miền, bao gồm:

1. *Root Name Servers*

Cũng thường được gọi là Name Server. Đây là Server quan trọng nhất trong hệ thống cấp bậc của DNS. Bạn cũng có thể hiểu rằng, Root Name Server chính là một thư viện để định hướng tìm kiếm giúp bạn.

Theo quy trình thực tế, sau khi nhận yêu cầu từ DNS Recursive Resolver, Root Name Server sẽ phản hồi rằng nó cần tìm trong các top-level domain name servers ( TLD Name Servers ) cụ thể nào.

1. *DNS Recursor*

Như đã nhắc đến ở trên, “cạ cứng” này đóng vai trò như một nhân viên cần mẫn, nhận nhiệm vụ lấy và trả thông tin về cho trình duyệt để tìm đúng thông tin mà chúng cần. Nói cách khác, DNS Recursor giữ trách nhiệm liên lạc với các Server khác để phản hồi đến trình duyệt người dùng. Tất nhiên là trong quá trình lấy thông tin, đôi khi nó cũng sẽ cần đến sự giúp đỡ của Root DNS Server.

1. *TLD Nameserver*

Khi bạn muốn truy cập Google hay Facebook, thường, phần mở rộng của bạn sẽ là “.com” đúng không? Vậy tôi muốn bạn biết rằng, nó chính là một trong các Top-level Domain đấy. Và Server cho loại Top-level domain này gọi là TLD Nameserver. Đây là nhà quản lý toàn bộ hệ thống thông tin của một phần mở rộng tên miền chung.

Theo trình tự, TLD Name Server sẽ phản hồi từ DNS Resolver, sau đó giới thiệu nó cho một Authoritative DNS Server – hay nơi chứa chính thức nguồn dữ liệu của tên miền đó.

1. *Authoritative Nameserver*

Khi DNS Resolver tìm thấy Authoritative Nameserver, đó là lúc mà việc phân giải tên miền diễn ra.

Mặt khác, Authoritative Name Server có chứa thông tin cho biết tên miền đang gắn với địa chỉ nào. Nó sẽ cung cấp cho Recursive Resolver địa chỉ IP cần thiết tìm thấy trong danh mục những bản ghi của nó.



1. **Sử dụng DNS như thế nào?**

Trong phần định nghĩa trên, ta có thể thấy được rằng các DNS Server đều có mối liên hệ với nhau. Đến đây thì nhiều bạn chắc chắn cũng sẽ “tẩu hỏa nhập ma” vì lăn tăn không biết nên sử dụng chúng như thế nào. Để tôi giúp bạn gỡ rối khoản này nhé!

Các Domain name system có tốc độ biên dịch khác nhau, bởi vậy, người dùng có thể tự lựa chọn DNS Server để sử dụng. Hoặc bạn có thể sử dụng DNS mặc định của nhà cung cấp dịch vụ Internet, hoặc dùng Domain Name Server miễn phí hoặc trả phí khác, đều được. Nhưng có một lưu ý là khi sử dụng các DNS Server khác, bắt buộc bạn phải thay đổi trong máy tính của mình.

Các bước thay đổi DNS trong máy tính

B1: Chọn Start – Setting – Network Connection

B2: Double click vào Local Area Connection, chọn Properties – Internet Protocol (TCP/IP) – Properties

B3: Điền thông số DNS Server bạn muốn vào 2 ô “Preferred DNS Server” & “Alternate DNS Server”.

*Lưu ý*

Các Hacker có thể thông qua DNS để đánh cắp những thông tin cá nhân của bạn. Vậy nên, hãy kiểm tra rõ tên truy cập của các Website, tránh truy cập vào các website giả mạo, các phần mềm không rõ nguồn gốc.

1. **Các loại bản ghi DNS là gì?**

***A Record***

* Là DNS Record đơn giản nhất, được sử dụng nhiều nhất để trỏ tên Website tới một địa chỉ IP cụ thể.
* Bạn có thể thêm một tên mới, thêm Time to Live ( thời gian tự động tái lại bản ghi ) và Points to ( Trỏ tới IP nào ).

***CNAME Record***

* Là bản ghi đóng vai trò như đặt một hoặc nhiều tên khác cho tên miền chính
* Bạn có thể tạo một tên mới, điều chỉnh trỏ tới tên gốc là gì và đặt TTL

***MX Record***

* Là bản ghi chỉ định Server nào quản lý các dịch vụ Email của tên miền đó
* Bạn có thể trỏ tên miền đến Mail Server, Đặt mức độ ưu tiên ( Priority ), đặt TTL

***TXT Record***

* Là bản ghi giúp bạn chứa các thông tin định dạng văn bản của tên miền
* Bạn có thể thêm host mới, giá trị TXT, TTL, Points to.

***AAAA Record***

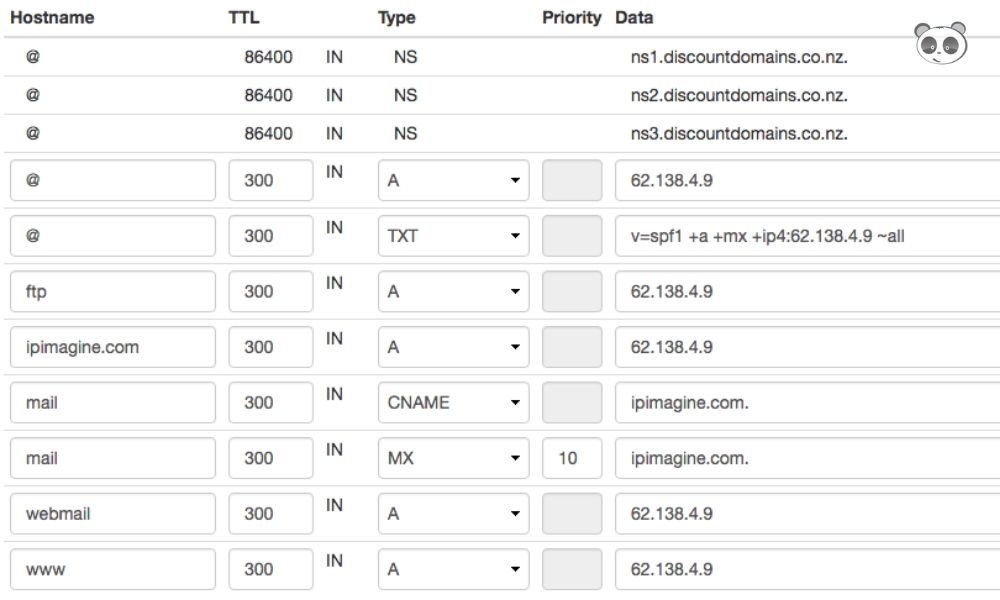
* Cùng là A Record, tuy nhiên, AAA Record được sử dụng để trỏ domain đến 1 địa chỉ IPV6 Address
* Bạn có thể thêm host mới, IPv6, TTL

***NS Record***

* Là DNS Server Records của tên miền, cho phép bạn chỉ định Name Server cho từng tên miền phụ
* Bạn có thể tạo host mới, tên Name Server, TTL

***SRV Record***

* Là bản ghi đặc biệt trong Domain Name System, dùng để xác định chính xác dịch vụ nào chạy port nào
* Bạn có thể thêm Priority, Name, Port, Points to,Weight, TTL.



1. **Tại sao DNS dễ bị tấn công?**

Quay lại phần Sử dụng DNS như thế nào, bạn có thấy một cảnh báo nhỏ của tôi về độ “mong manh, dễ vỡ” và dễ bị tấn côngkhông? Để tôi lý giải giúp bạn tại sao nhé!

Quá trình tên miền được dịch thành địa chỉ IP, được gọi là phân giải DNS.

Khi ai đó nhập một tên miền nào đó, chẳng hạn www.google.com vào Web Browser, thì trình duyệt lập tức liên hệ với 1 máy chủ tên, để lấy địa chỉ IP tương ứng. Có 2 loại máy chủ tên:

Máy chủ tên có thẩm quyền: Nơi lưu trữ thông tin đầy đủ về một vùng

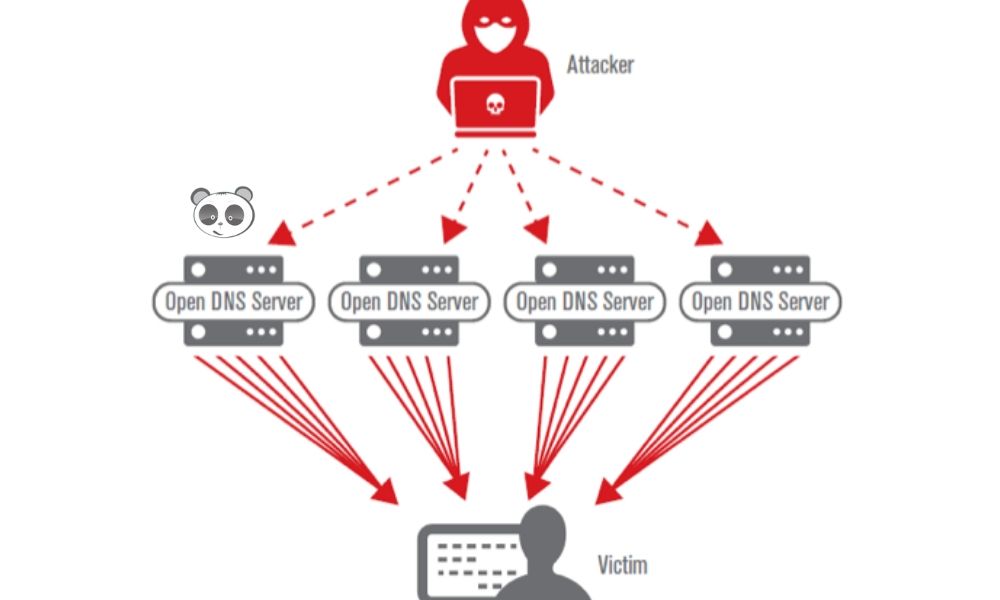
Máy chủ tên đệ quy: Nơi trả lời các truy vấn DNS cho người dùng Internet, đồng thời lưu trữ kết quả phản hồi của DNS trong một khoảng thời gian.

Vậy thì vấn đề mà chúng ta đang muốn nhấn mạnh, nằm ở bộ máy chủ tên đệ quy.

Khi một máy chủ đệ quy nhận được phản hồi, nó sẽ lưu vào bộ nhớ tạm phản hồi đó, để tăng tốc độ của các truy vấn tiếp theo. Ưu điểm của việc lưu trữ là sẽ giảm số lượng yêu cầu thông tin cần thiết, nhưng đồng thời cũng phát sinh một rủi ro “đáng gờm” là dễ bị tấn công bởi man-in-the-middle, tạm dịch là người trung gian.

Thông quan các màn battle “ngoài sáng trong tối” này, tội phạm mạng sẽ có thể:

* Cướp Email
* Can thiệp Voice Over IP ( VoIP )
* Mạo danh các trang web
* Đánh cắp thông tin đăng nhập và mật khẩu
* Trích xuất dữ liệu thẻ tín dụng và một số thông tin mật khác



1. **Danh sách DNS phổ biến nhất hiện nay**

***Google Public DNS Server***

Đây là một trong những DNS Server nhanh nhất, và đặc biệt được nhiều người dùng sử dụng nhất. Với DNS Server của Google, bạn sẽ có trải nghiệm duyệt Web tốt hơn, đồng thời độ bảo mật cũng cao hơn.

→ Để sử dụng Google Public DNS Server, hãy thay cấu hình cài đặt hệ thống mạng của bạn bằng địa chỉ IP dưới đây:

* *Preferred DNS server: 8.8.8.8*
* *Alternate DNS server: 8.8.4.4*



***OpenDNS***

Nếu bạn đang tìm kiếm máy chủ Domain name system công cộng tốt nhất, thậm chí là không có thời gian chết, thì OpenDNS là option bạn không thể bỏ qua.

Dựa trên nền tảng đám mây, OpenDNS cũng là một trong các DNS Server nhanh nhất, có lẽ chỉ xếp sau DNS Server của Google. Hệ thống này sẽ bảo vệ tối đa cho máy tính của bạn trước những cuộc tấn công trên mạng Internet.

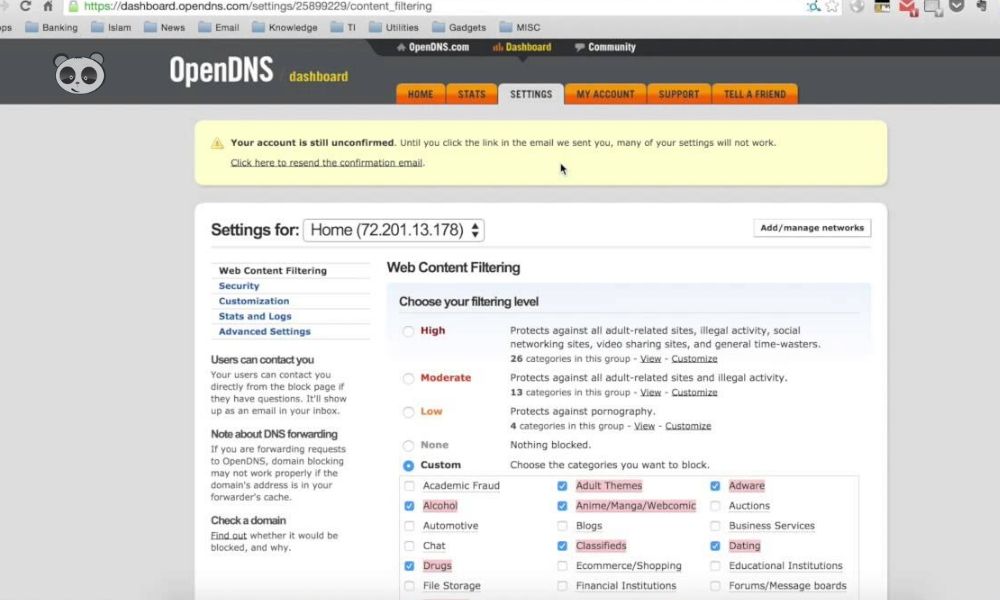
→ Để sử dụng OpenDNS Server, hãy thay cấu hình cài đặt hệ thống mạng của bạn bằng địa chỉ IP dưới đây:

* *208.67.222.222*
* *208.67.222.220*

Ngoài ra, OpenDNS cũng cung cấp 2 giải pháp miễn phí cho người dùng tuỳ chỉnh bao gồm: OpenDNS Family Shield (Cấu hình sẵn để chặn nội dung người lớn) và OpenDNS Home (đi kèm bộ lọc tuỳ chỉnh, bảo vệ máy tính của bạn khỏi hacker và phishing).

→ Cấu hình cài đặt hệ thống mạng để sử dụng OpenDNS Family Shield:

* *Preferred DNS server: 208.67.222.123*
* *Alternate DNS server: 208.67.220.123*



***Comodo Secure DNS***

Là một trong những Public DNS Server tốt nhất Comodo Secure DNS cung cấp trải nghiệm duyệt web “đỉnh” hơn rất nhiều so với những nhà cung cấp dịch vụ Internet “cùi bắp”. Bạn có thể lướt tất cả các trang web một cách dễ dàng và hoàn toàn an toàn mà không cần phải cài đặt bất kỳ phần cứng hoặc chương trình hỗ trợ thứ 3 nào cả!

→ Để sử dụng Comodo Secure DNS, hãy thay cấu hình cài đặt hệ thống mạng của bạn bằng địa chỉ IP dưới đây:

* Primary DNS Server: 8.26.56.26
* Secondary DNS Server: 8.20.247.20