Tổng quan về DNS

Internet bao gồm hàng tỷ máy tính kết nối mạng với nhau, mỗi máy tính cần có một địa chỉ IP. Địa chỉ IPv4 có 32 bit đang được sử dụng phổ biến hiện nay, mỗi phần là 8 bits (1 byte) cách đếm từ trái qua phải, mỗi phần cách nhau bởi một dấu chấm và nếu ở dạng thập phân đây đủ là 12 số.

Ví dụ máy chủ web server của công ty X có địa chỉ: 123.123.123.123 và tên miền của nó là x.com.vn. Thực tế người dùng muốn truy cập đến trang chủ của công ty X thì không cần biết đến địa chỉ IP mà chỉ cần tên miền của nó. Hệ thống tên miền sẽ trả lời lại địa chỉ IP cho máy tính của người dùng.

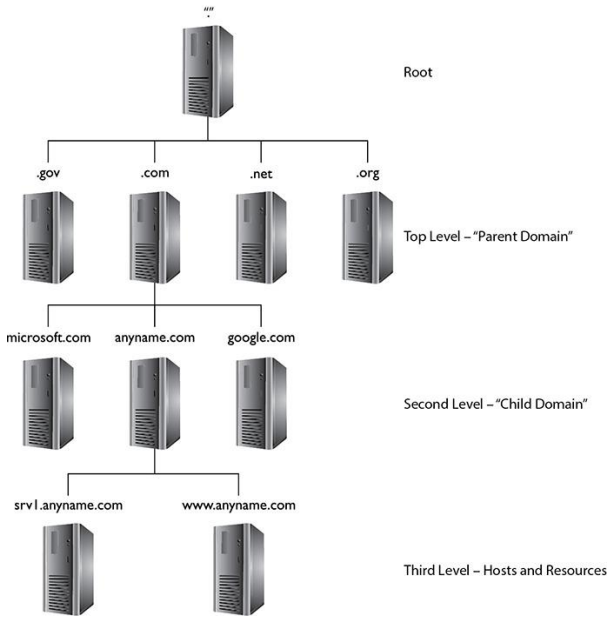
I. Hệ thống tên miền (Domain name system)

Hệ thống tên miền bao gồm một loạt các cơ sở dữ liệu chứa địa chỉ IP và các tên miền tương ứng của các địa chỉ IP. Mỗi tên miền ứng với địa chỉ IP cụ thể. Hệ thống tên miền trên mạng Internet có nhiệm vụ chuyển đổi tên miền sang địa chỉ IP và ngược lại.

Mục đích đem lại sự tiện lợi trong việc truy cập websites của người dùng.

II. Cấu trúc hệ thống tên miền

Cơ sở dữ liệu hệ thống DNS là hệ thống cơ sở dữ liệu phân tán và phân cấp hình cây như hình dưới đây.



Với root server là đỉnh của cây và sau đó là các miền (domain) được phân nhánh dần xuống dưới và phân quyền quản lý. Khi một máy khách truy vấn một tên miền, nó sẽ đi lần lượt từ root phân cấp xuống dưới để đến DNS quản lý domain cần truy vấn.

Tên miền được phân nhánh thành nhiều cấp như:

- Domain root: Đỉnh của cây tên miền. thể hiện bằng dấu chấm
- Tên miền cấp 1: Gồm vài ký tự xác định một nước, khu vực hoặc tổ chức. Ví dụ: .com
- Tên miền cấp 2: Tên công ty hoặc tổ chức. Ví dụ: bkacad.com
- Sub-domain: Tên được sử dụng như chi nhánh, phòng ban của một cơ quan. Ví dụ: tuyensinh.bkacad.com

III. Máy chủ DNS

Máy chủ DNS là 1 máy tính chạy chương trình các chương trình quản lý DNS như: DNS Server Service hay BIND: Berkeley Internet Name Domain.

Primary name server : là DNS server chính, trên đó cho phép thêm, xóa sửa CSDL của DNS.

Secondary name sever: là DNS server phụ, backup lại CSDL của Primary. Không được thay đổi CSDL DNS. - Khi Primary name server bị fail, Secondary được sử dụng để phân giải tên. Hoặc Primary quá tải nó sẽ chuyển bớt qua cho Secondary. Khi Primary có thay đổi thì Secondary sẽ update thông tin từ Primary Server và lưu trữ nó.

Có hai giải pháp lấy thông tin về các Zone mới :

- full: lấy toàn bộ
- incremental: chỉ lấy phần thay đổi

Caching Name Server: DNS Server và Client sẽ lưu lại những truy vấn (caching)

Để khi được truy vấn lần sau nó sẽ tìm trong cache trước, nếu cache có nó sẽ trả lời ngay lập tức mà không cần truy vấn nữa. Điều này giúp cho mạng hoạt động nhanh hơn (tăng performing).

```
ipconfig /dnsflush

ipconfig /displaydns
```

Caching-only không chứa Zone nào và cũng không có quyền quản lý bất kì domain nào. Nó sử dụng bộ cache của mình để lưu các truy vấn của DNS của Client giúp:

- Làm tăng tốc độ phân giải bằng cách sử dụng cache.
- Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
- Giảm việc lưu thông trên những mạng lớn.

IV. Zone

Những domain và subdomain mà DNS Server quản lý gọi là Zone.

=> 1 zone có thể gồm 1 domain, 1 hoặc nhiều subdomain

DNS cho phép chia hệ thống tên miền thành Zone và trong Zone quản lý tên miền được phân chia đó. Các Zone chứa thông tin vê miền cấp thấp hơn, có khả năng chia thành các Zone cấp thấp hơn và phân quyền (delegation control) cho các DNS Server khác quản lý.

Zone file DNS là đại diện của zone DNS - chứa tất cả các bản ghi cho một miền cụ thể. Trong đó, mỗi dòng chỉ có thể giữ một bản ghi và phải bắt đầu bằng giá trị TTL (Thời gian tồn tại), chỉ định thời gian lưu giữ các bản ghi trong bộ đệm của Máy chủ DNS. Bản ghi bắt buộc khác cho zone file DNS là bản ghi - nó chỉ định máy chủ tên chính thức cho Vùng DNS.

```
$ORIGIN example.com. ; designates the start of this zone file in the name space

$TTL 1h ; The default expiration time of a resource record without its own TTL value

example.com. IN SOA ns.example.com. root.example.com. (

2008120710 ; serial number of this zone file

1d ; slave refresh (1 day)

1d ; slave retry time in case of a problem (1 day)

4w ; slave expiration time (4 weeks)

1h ; minimum caching time in case of failed lookups (1 hour)

)

example.com. NS dns1.ntchosting.com. ; ns.example.com is the nameserver for example.com

example.com. NS dns2.ntchosting.com. ; ns.somewhere.com is a backup nameserver for example.com
```

```
example.com. MX 10 mx1.ntchosting.com

example.com. MX 10 mx2.ntchosting.com ; mail.example.com is the mailserver for example.com

example.com. A 209.25.134.47 ; ip address for "example.com"

www A 209.25.134.47
```

V. Các bản ghi thường có trong CSDL của DNS server

Bản ghi SOA (Start of Authority): Bản ghi này xác định máy chủ DNS có thẩm quyền cung cấp thông tin về tên miền xác định trên DNS.

Nội dung bản ghi SOA như sau:

- Source host: Tên máy chủ DNS chính của zone (cần liên quan tới bản ghi NS)
- Contact e-mail: Địa chỉ email liên lạc của người chị trách nhiệm về zone file
- Serial number: Số lần sửa đổi của zone file. Con số này tăng lên mỗi khi zone file được hay đổi và được sử dụng bởi secondary DNS server để biết khi nào cập nhật bản sao từ primary DNS server.
- Refesh time: Thời gian mà secondary DNS server sẽ đợi trước khi yêu cầu cập nhật. Giá trị mặc định là 3600s.
- Retry time: Thời gian mà DNS server sẽ đợi nếu quá trình zone transfer bị lỗi. Giá trị mặc định là 600s.
- Expire time: Thời gian tối đa mà DNS server dùng để hoàn tất zone transfer. Giá trị mặc định là 86400s.
- TTL: Giá trị tồn tại của tất cả các bàn ghi trong zone. Nếu không được cập nhật bởi zone transfer, các bản ghi sẽ bị xóa bỏ. Giá trị mặc định là 3600s.

Bản ghi A: Bản ghi kiểu A được dùng để khai báo ánh xạ giữa tên của một máy tính trên mạng và địa chỉ IP của một máy tính trên mạng. Bản ghi kiểu A có cú pháp như sau:

Domain IN A <IP address>

Ví dụ:

home.bkacad.com IN A 123.123.123.123

Theo ví dụ trên, tên miền home.bkacad.com được khai với bản ghi kiểu A trỏ đến địa chỉ 123.123.123.123 sẽ là tên của máy tính này. Một tên miền có thể được khai

nhiều bản ghi kiểu A khác nhau để trỏ đến các địa chỉ IP khác nhau. Như vậy có thể có nhiều máy tính có cùng tên trên mạng. Ngược lại một máy tính có một địa chỉ IP có thể có nhiều tên miền trỏ đến, tuy nhiên chỉ có duy nhất một tên miền được xác định là tên của máy, đó chính là tên miền được khai với bản ghi kiểu A trỏ đến địa chỉ của máy.

Bản ghi CNAME: Bản ghi CNAME cho phép một máy tính có thể có nhiều tên. Nói cách khác bản ghi CNAME cho phép nhiều tên miền cùng trỏ đến một địa chỉ IP cho trước. Để có thể khai báo bản ghi CNAME , bắt buộc phải có bản ghi kiểu A để khai báo tên của máy. Tên miền được khai báo trong bản ghi kiểu A trỏ đến địa chỉ IP của máy được gọi là tên miền chính (canonical domain).Các tên miền khác muốn trỏ đến máy tính này phải được khai báo là bí danh của tên máy (alias domain). Cú pháp của bản ghi này như sau:

alias-domain IN CNAME canonical-domain

Ví dụ:

www.bkacad.com IN CNAME home.bkacad.com

Tên miền www.bkacad.com sẽ là tên bí danh của tên miền home.bkacad.com , hai tên miền sẽ cùng trỏ đến địa chỉ IP 123.123.123.123

Bản ghi MX: dùng để khai báo trạm chuyển tiếp thư điện tử của một tên miền.

Ví dụ : Để các thư điện tử có cấu trúc user@bkacad.com được gửi đến trạm chuyển tiếp thư điện tử có tên mail.bkacad.com, trên cơ sở dữ liệu cần khai báo bản ghi MX như sau:

bkacad.com IN MX 10 mail.bkacad.com

Các thông số được khai báo trong bản ghi MX nêu trên gồm có:

- bkacad.com: là tên miền được khai báo để sử dụng như địa chỉ thư điện tử.
- mail.bkacad.com: là tên của trạm chuyển tiếp thư điện tử, nó thực tế là tên của máy tính dùng làm máy trạm chuyển tiếp thư điện tử.
- 10: Là giá tri ưu tiên, giá trị ưu tiên có thể là một số nguyên bất kì từ 1 đến 225, nếu giá trị ưu tiên này càng nhỏ thì trạm chuyển tiếp thư điện tử được khai báo sau đó sẽ là trạm chuyển tiếp thư điện tử được chuyển đến đầu tiên.

Ví dụ nếu khai báo :

bkacad.com IN MX 10 mail. bkacad.com

bkacad.com IN MX 20 backupmail. bkacad.com

Thì tất cả các thư điện tử có cấu trúc địa chỉ user@ bkacad.com trước hết sẽ được gửi đến trạm chuyển tiếp thư điện tử mail. bkacad.com.Chỉ trong trường hợp máy chủ mail. bkacad.com không thể nhận thư thì các thư này mới chuyển đến trạm chuyển tiếp thư điện tử backupmail. bkacad.com.

Bản ghi PTR: Hệ thống DNS không những thực hiện việc chuyển đổi từ tên miền sang địa chỉ IP mà còn thực hiện chuyển đổi địa chỉi IP mà còn thực hiện chuyển đổi địa chỉ IP sang tên miền. Bản ghi PTR cho phép thực hiện chuyển đổi địa chỉ IP sang tên miền. Cú pháp của bản ghi PTR:

123.123.123.123.in-addr.arpa IN PTR www.bkacad.com

Bản ghi PTR trên cho phép tìm tên miền www.bkacad.com khi biết địa chỉ IP (123.123.123.123) mà tên miền trỏ tới.

Bản ghi NS: xác định một máy chủ tên miền có thẩm quyền. Máy chủ DNS này chứa thông tin của các domain.

Cú pháp : domain IN NS DNS-Server