B

bloodplanet
Wh------

21/03/2015

7

51 bài viết

B bloodplanet · 25/03/2015 · 10.429 Lượt xem

[h=1]DỊCH VỤ TÊN MIỀN - DNS (Domain Name Service hoặc Domain Name System)[/h]Cá nhân mỗi con người có thể được xác định theo nhiều cách. Ví dụ, chúng ta có thể được nhận biết qua tên trong giấy khai sinh, bằng số chứng minh thư nhân dân. Dù có nhiều cách nhận biết để phân biệt mọi người nhưng phương thức nhận biết nào phụ thuộc vào hoàn cảnh. Ví dụ công an sử dụng số chứng minh thư nhân dân chứ không sử dụng tên. Bình thường mọi người thích nhớ tên nhau hơn là số chứng minh thư.

Giống như con người, máy tính trên Internet cũng có thể được xác định bằng nhiều cách. Tên máy tính (host name) và một cách, ví dụ cnn.com, www.yahoo.com, gais.umass.edu hay surf.eurecom.fr. Những tên đó tương đối dễ nhớ đối với con người. Tuy nhiên tên máy tính cung cấp ít thông tin về vị trí trên Internet của máy tính (tên máy tính surf.eurecom.fr chỉ cho chúng ta biết máy tính đó ở nước Pháp vì kết thúc bằng đuôi .fr, ngoài ra không còn thông tin nào khác). Hơn nữa tên máy tính bao gồm nhiều ký tự - cả chữ cái và chữ số - có độ dài thay đổi nên router khó có thể xử lý được. Vì lý do đó, máy tính được xác định thông qua địa chỉ IP. Địa chỉ IP gồm có 4 byte và có cấu trúc phân cấp, giá trị của mỗi byte sẽ được đổi ra số thập phân (0-255) và cách nhau bằng dấu chấm (ví dụ 121.23.45.5). Địa chỉ IP phân cấp vì khi duyệt địa chỉ từ trái qua phải, chúng ta nhận được thêm nhiều thông tin xác đinh về vị trí của máy tính trên Internet (vị trí ở trong mạng của các mạng, trong một mạng…). Điều này tương tự khi xét địa chỉ bưu điện từ dưới lên, chúng ta nhận được nhiều thông tin về địa chỉ đó.

[h=1]1. Các dịch vụ của DNS[/h]Có hai cách để xác định một máy tính: dựa vào tên máy tính hoặc địa chỉ IP. Con người thích sử dụng tên máy dễ nhớ, trong khi router lại sử dụng địa chỉ IP có cấu trúc phân cấp và độ dài cố định (dễ xử lý). Để dung hoà giữa hai cách, chúng ta cần một dịch vụ chỉ dẫn để chuyển đổi tên máy tính sang địa chỉ IP và đây chính là nhiệm vụ của hệ thống tên miền trên Intemet (DNS). DNS là (1) Cơ sở dữ liệu phân tán được đặt trên một hệ thống phân cấp các máy phục vụ tên (nameserver) và (2) Giao thức thuộc tầng ứng dụng cho phép máy tính và máy chủ tên trao đổi thông tin phục vụ mục đích xác định địa chỉ IP. Máy chủ tên thường là các máy UNIX sử dụng phần mềm Berkely Internet Name Domain (BIND). Giao thức DNS chạy trên nền UDP với số hiệu cổng là 53.

Thông thường DNS được các giao thức tầng ứng dụng khác như HTTP, SMTP và FTP sử dụng để xác định địa chỉ IP từ tên máy tính do người dùng đưa vào. Chuyện gì xảy ra khi trình duyệt (HTTP client) trên máy tính của người sử dụng yêu cầu đối tượng có địa chỉ URL là www.someschool.edu.index.html. Để gửi được thông điệp HTTP yêu cầu tới Web server thì máy tính của người sử dụng phải xác định được địa chỉ IP của www someschool.edu. Điều này được thực hiện như sau: máy tính của người sử dụng chạy phía client của ứng dụng DNS. Trình duyệt sẽ lấy ra tên máy tính (www.someschool.net) từ địa chỉ URL và chuyển nó cho phần mềm client của DNS. DNS client gửi một truy vấn (query) chứa tên máy tính tới DNS server. DNS client sẽ nhận được một thông điệp trả lời từ DNS server chứa địa chi IP cần xác định. Sau đó trình duyệt sẽ mở một kết nối TCP tới tiến trình HTTP server trên máy tính có địa chỉ IP vừa được xác định.

Rõ ràng các ứng dụng Internet sử dụng DNS hoạt động chậm đi. Tuy nhiên, địa chỉ IP đã được xác định thường được ghi tạm (cache) trong một name server DNS ở gần và như vậy làm giảm tải cho hệ thống DNS cũng như độ trễ của ứng dụng.

Bên cạnh dịch vụ xác định địa chỉ IP từ tên máy, DNS cung cấp một số dịch vụ quan trọng sau:

[h=2]1.1. Dịch vụ đặt bí danh cho máy tính (Host aliasing)[/h]Máy tinh có tên phức tạp có thể có một hoặc nhiều bí danh (alias). Ví dụ tên máy tính relay1.west-coast.enterprise.com có thể có hai bí danh là www.enterprise.com và enterprise.com. Trong trường hợp này, relay1.west-coast.enterprise.com là tên đầy đủ (canonical name). Tên bí danh thường dễ nhớ hơn tên đầy đủ. Một ứng dụng có thể yêu cầu DNS xác định tên đầy đủ cũng như địa chỉ IP của một tên bí danh.

[h=2]1.2. Dịch vụ đặt bí danh cho mail server (Mail server aliasing)[/h]Hiển nhiên địa chỉ mail cần dễ nhớ. Ví dụ nếu Bob có tài khoản trên Hotmail, địa chỉ của Bob có thể chỉ đơn giản là bob@hotmail.com. Tuy nhiên tên máy tính của máy phục vụ thư tại Hotmail phức tạp và vì thế khó nhớ hơn so với hotmail.com (ví dụ tên đầy đủ có thể là relay1.west-coast.hotmail.com). ứng dụng có thể sử dụng DNS để xác định tên đầy đủ của một bí danh cũng như địa chỉ IP của máy tính đó. Trên thực tế, DNS cho phép mail server và webserver của các công ty có tên (bí danh) giống nhau, ví dụ: webserver và mail server của một công ty có thể cùng là enterprise.com.

[h=2]1.3. Phân tán tải (load distribution)[/h]DNS thực hiện việc phân tán tải cho các server, đặc biệt là các web server nhân bản (replicated - là các server có nội dung giống hệt nhau). Những site có nhiều người truy cập như cnn.com được đặt trên nhiều server giống hệt nhau. Mỗi server là một hệ thống đầu cuối (end system) khác nhau, có địa chỉ IP khác nhau. Đối với các server giống hệt nhau như vậy, một nhóm địa chỉ IP sẽ gắn với tên đầy đủ của một máy nào đó. Cơ sở dữ liệu DNS chứa toàn bộ nhóm địa chỉ IP đó. Khi client gửi truy vấn DNS để xác định địa chỉ IP thì server sẽ gửi toàn bộ nhóm địa chỉ IP đó nhưng server thay

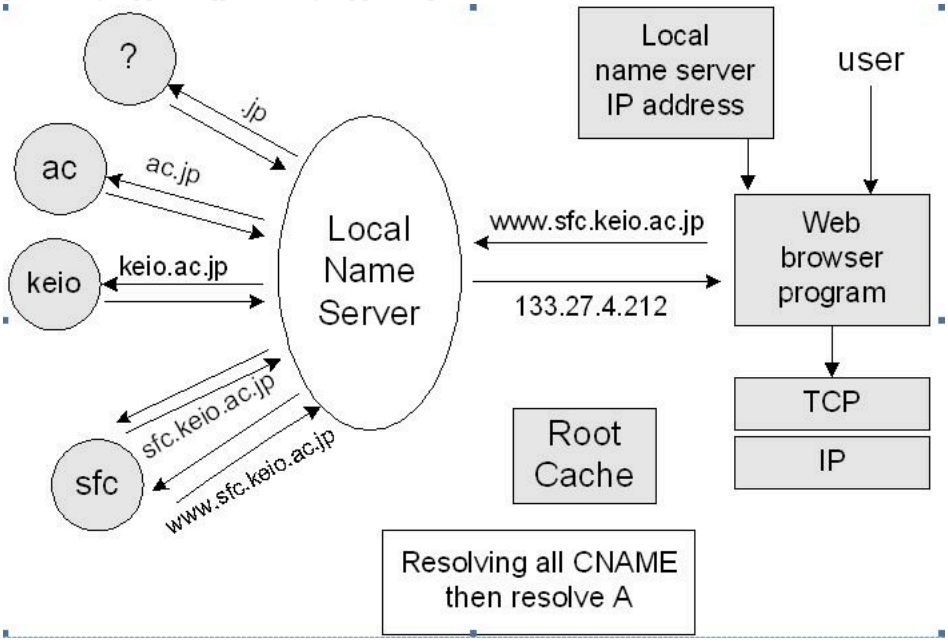
DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS

ở dụng cho email khi nhiều mail server có chung bí danh.

[h=1]DNS: Một dịch vụ mạng quan trọng hoạt động trên mô hình client/server.[/h]Giống HTTP, FPT hay SMTP, giao thức DNS nằm ở tầng ứng dụng vì (1) nó hoạt động giữa hai thực thể truyền thông đầu cuối sử dụng mô hình client/server và (2) sử dụng một giao thức giao vận end-to-end ở tầng giao vận phía dưới để trao đổi thông điệp DNS giữa hai phía đầu cuối. Tuy nhiên vai trò của DNS khác các ứng dụng Web, FTP hay Email nhiều. DNS không phải ứng dụng được người dùng trực tiếp sử dụng mà DNS chỉ cung cấp một dịch vụ Internet cực kỳ thiết yếu cho các ứng dụng: chuyển đổi tên máy tính sang địa chỉ IP. Sự phức tạp trong kiến trúc của Internet được đặt tại “lớp vỏ” của mạng. DNS được triển khai trên các máy tính đầu cuối là một minh chứng rõ ràng cho nguyên lý thiết kế này.

[h=1]2. Cơ chế hoạt động tổng quan của DNS.[/h]Bây giờ, chúng ta trình bày tổng quan cách thức hoạt động của DNS, tập trung vào dịch vụ xác định địa chỉ IP từ tên máy tính. Với client, DNS là một "hộp đen". Client gửi thông điệp truy vấn DNS vào hộp đen đó, trong thông điệp chứa tên máy cần xác định địa chỉ IP. Với hệ điều hành Unix, gethostname() là một hàm mà ứng dụng có thể gọi để gửi thông điệp truy vấn. Sau một khoảng thời gian nào đó - từ vài phần nghìn giây đến vài chục giây, client nhận được thông điệp trả lời của DNS chứa địa chỉ IP cần xác định. Vì vậy, với client thì DNS là một dịch vụ xác định IP đơn giản và dễ hiểu. Nhưng "hộp đen" triển khai dịch vụ đó thực sự phức tạp, bao gồm nhiều máy chủ tên (nameserver) đặt khắp nơi trên thế giới và một giao thức ở tầng ứng dụng xác định cách thức trao đổi thông tin giữa các nameserver và giữa nameserver và máy tính.

[FONT=&quot] [/FONT][FONT=&quot] [/FONT]



Hình 1 Ứng dụng sử dụng dịch vụ của DNS

Để triển khai DNS, người ta có thể đưa ra một kiến trúc đơn giản sau: có một nameserver chứa tất cả các ánh xạ tên và địa chỉ IP. Theo thiết kế tập trung này, client chỉ cần gửi tất cả các truy vấn tới nameserver duy nhất và nameserver này sẽ trực tiếp trả lời mọi truy vấn. Mặc dù tính đơn giản của thiết kế này rất hấp dẫn nhưng nó hoàn toàn không thích hợp cho Intemet với số lượng lớn và ngày càng tăng các máy tính. Thiết kể tập trung như vậy nảy sinh một số vấn đề sau:

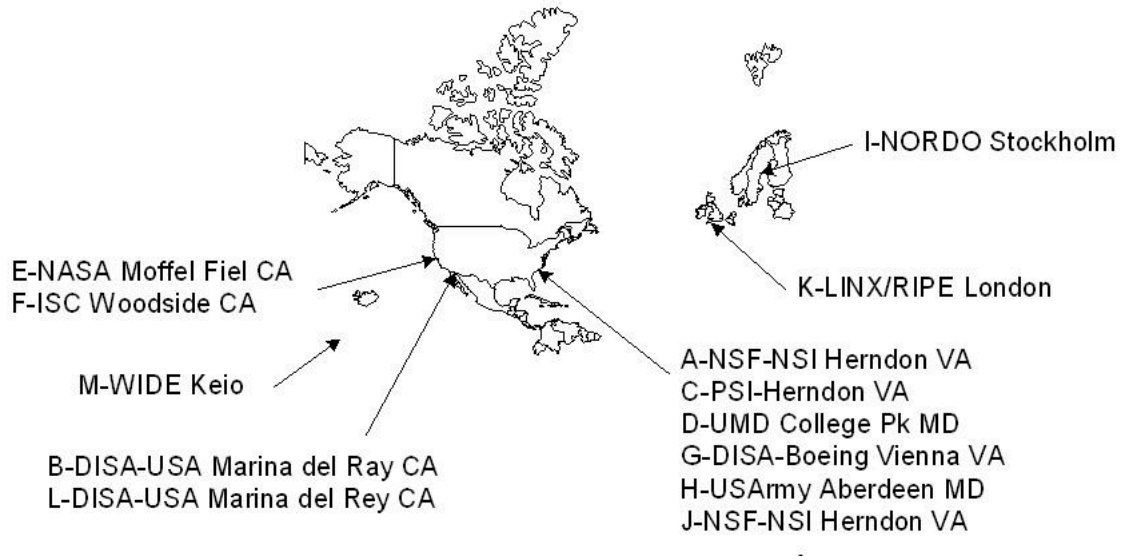
- **Điểm hỏng duy nhất (A single point of failure)** nếu nameserver duy nhất ngừng làm việc cũng có nghĩa là toàn bộ Internet ngừng hoạt động.
- **Khối lượng lưu lượng (Traffic volume):** Một nameserver duy nhất phải xử lý tất cả các truy vấn DNS (cho tất cả các thông điệp yêu cầu từ hàng triệu máy tính trên toàn cầu)
- **Cơ sở dữ liệu tập trung ở xa (distant centralized database):** Nameserver duy nhất không thể gần tất cả các client. Nếu nameserver đặt ở NewYork thì tất cả truy vấn từ Úc phải chuyển tới phía bên kia trái đất và có thể qua một đường kết nối chậm và tắc nghẽn. Hậu quả là các ứng dụng phải chịu độ trễ lớn.
- **Bảo trì (maintenance):** Namserver phải ghi nhớ thông tin về tất cả các máy tính trên Intemet. Khi đó cơ sở dữ liệu sẽ cực kỳ lớn và nameserver phải cập nhật thường xuyên thông tin cho mọi máy tính mới. Cũng phải giải quyết các vấn đề kiểm chứng và xác nhận khi người dùng sử dụng cơ sở dữ liệu tập trung.

Tóm lại, một cơ sở dữ liệu tập trung trên một nameserver duy nhất không phù hợp khi quy mô hệ thống lớn. Do đó, DNS được thiết kế phân tán. Trên thực tế DNS là một ví dụ tuyệt vời về triển khai cơ sở dữ liệu phân tán trên Internet. Để giải quyết vấn đề quy mô, DNS sử dụng nhiều nameserver tổ chức phân cấp và phân tán trên toàn cầu. Không có nameserver nào chứa tất cả tên và địa chỉ IP các máy tính trên Internet những thông tin này được phân tán trên nhiều nameserver. Có ba loại nameserver chính: local nameserver, root nameserver và authoritative nameserver. Các nameserver đó trao đổi thông tin với nhau và với các máy tính khác.

- **Local nameserver**: Mỗi ISP như trường đại học khoa thuộc trường, công ty đều có local nameserver (còn được gọi là default

địa chỉ IP của local name server bằng cách mở Control Panel, sau đó chọn Network, chọn TCP/IP, rồi chọn cấu hình DNS). Loại name server thường "gần" với client, trong trường hợp tại cơ quan của một tổ chức, nó có thể ở trên cùng mạng LAN với máy tính client. Với ISP phục vụ kết nối từ nhà thì khoảng cách giữa name server và các máy tính client chỉ là vài router. Nếu máy tính yêu cầu xác định địa chỉ IP của một máy tính khác trong cùng một ISP thì local name server có thể ngay lập tức xác định được địa chi IP cần thiết. Ví dụ nếu máy tính surf.eurecom.fr yêu cầu địa chỉ áp của baie.eurecom.fr thì local name server ở eurecom ngay lập tức có thể đưa ra địa chỉ IP được yêu cầu mà không phải liên hệ với bất kỳ name server nào khác.

- **Rootname server** : Trên Intemet có 13 rootname server, hầu hết đặt tại Bắc Mỹ. Vị trí các root name server vào thời điểm tháng 02/1998 được minh hoạ trên hình 2. Khi local name server không thể trả lời truy vấn của một máy tính (bởi vì nó không có thông tin của máy tính được yêu cầu) thì local name server sẽ đóng vai trò client DNS và gửi câu hỏi truy vấn tới một trong số các root name server. Nếu root name server có thông tin của máy tính được hỏi, nó sẽ gửi một thông điệp hồi âm DNS tới local name server và sau đó thông tin này được local name server gửi trả lời cho máy tính yêu cầu. Nhưng root name server có thể không có thông tin của máy tính đó (và thường là không có). Trong trường hợp này, root name server biết được địa chỉ IP của name server quản lý máy tính đó.

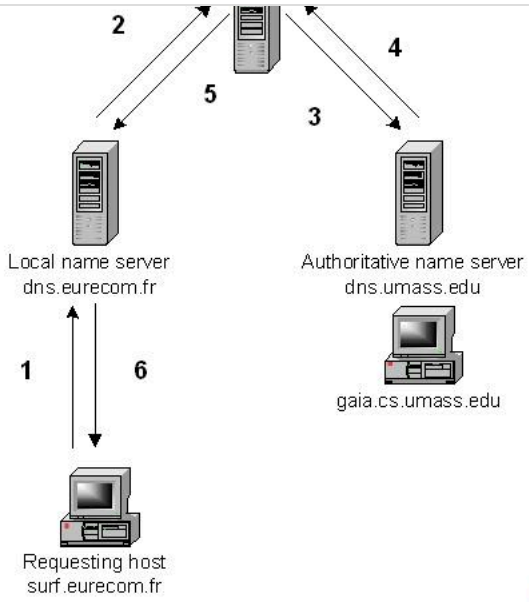


Hình 2 Các root name server trên thế giới

- **Authoriative name server**: Mỗi máy tính phải đăng ký tới một Authoritative name server. Thông thường authoriative name server của một máy tính là name server trong miền ISP của máy tính đó (thực tế mỗi máy tính phải có ít nhất hai authoritative name server, để đề phòng trường hợp một name server bị hỏng). Có thể định nghĩa, Authoriative name server của một máy tính là nameserver luôn lưu trữ bản ghi DNS cho phép xác định địa chỉ IP của máy tính đó từ tên. Khi authoritative name server nhận được truy vấn từ root nameserver, nó sẽ gửi một thông điệp DNS trả lời chứa ánh xạ được yêu cầu. Sau đó, root server gửi ánh xạ đó tới local nameserver và local nameserver lại tiếp tục gửi ánh xạ đó tới máy tính yêu cầu. Nhiều nameserver vừa là local vừa là authoriative nameserver.

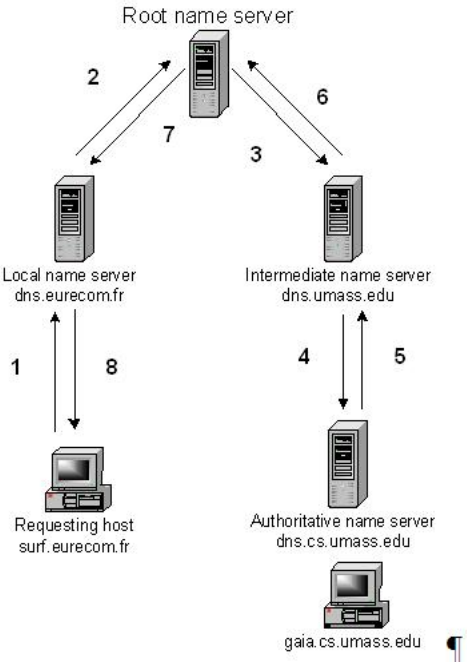
Xét ví dụ đơn giản sau. Giả sử máy tính surf.eurecom.fr muốn có địa chỉ IP của máy tính gaia.cs.umas.edu, giả sử nameserver của miền Eurecom là dns.eurecom.com.fr và authoriative nameserver cho gaia.cs.umas.edu là dns.umass.edu. Như đã trình bày trong hình 3, đầu tiên máy tính surf.eurecom.fr gửi một thông điệp truy vấn tới local name server của nó là dns.eurecom.fr. Thông điệp đó chứa tên máy tính cần xác định địa chỉ IP, là gaia.cs.umass.edu. Loal name server gửi thông điệp tới root name server. Root nameserver gửi tiếp thông điệp tới nameserver có thể xác định tất cả các máy tính trong miền umass.edu, ví dụ là dns.umass.edu. Sau đó, authoriative name server này gửi kết quả cho cho surf.eurecom.fr thông qua root name server và local name server. Trong ví dụ này, để xác định được địa chỉ IP, có 6 thông điệp DNS được trao đổi : 3 thông điệp yêu cầu và 3 thông điệp trả lời.

DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS



Giả thiết root name server biết địa chỉ IP của authoriative name server của mọi máy tính như trên có thể không đúng. Với tên một máy tính, root nameserver có thể chỉ biết được địa chỉ IP của một name server trung gian mà chính name server trung gian này mới biết được địa chỉ IP của authoriative nameserver của máy tính đó. Để minh hoạ điều vẫn xét ví dụ trên máy tính surf.eurecom.fr cần xác định địa chỉ IP của gai.cs.umass.edu. Giả sử trường Đại học Massachusets (Univ of Massachusets) có name server cho toàn bộ trường đại học, đó 1à dns.umass.edu. Ta cũng giả sử tiếp rằng mỗi khoa trong trường Đại học này có name server riêng, quản lý tên cho tất cả các máy tính trong khoa đó. Khi root name server nhận được yêu cầu xác định địa chỉ IP cho một tên máy tính có tận cùng 1à umass.edu, nó sẽ gửi yêu cầu tới name server dns.umass.edu. Name server này gửi tất cả các yêu cầu có tên máy tính tận cùng là cs.umass.edu cho authoritative name server quản lý tất cả máy tính có tên tận cùng là cs.umass.edu. Authoriative name server này (dns.cs.umass.edu) gửi kết quả tới name server trung gian (dns.umass.edu) và name server này sẽ gửi tiếp kết quả tới root name server. Root name server sẽ gửi tiếp kết quả tới local name server của máy tính yêu cầu. Trong ví dụ này, 8 thông điệp DNS được gửi (Hình 4). Thực ra có thể có nhiều hơn 8 thông điệp DNS được trao đổi vì có thể có nhiều name server trung gian ở giữa root name server và authoriative name server.

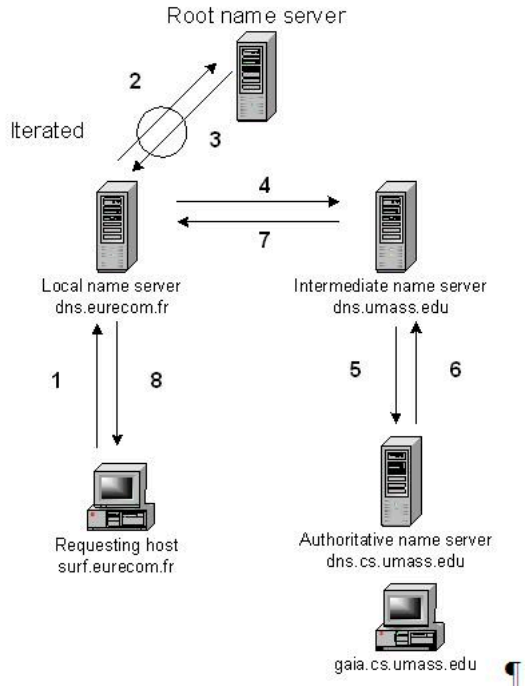
Trong ví dụ trên, tất cả các truy vấn được là đệ quy (recursive query). Khi máy tính hay name server A gửi thông điệp yêu cầu tới name server B, name server B sẽ thay mặt A nhận thông điệp chứa kết quả và sau đó gửi kết quả tới A. Tuy nhiên DNS cho phép các truy vấn tương tác (iterative query) ở bất kì giai đoạn nào trong quá trình từ máy tính yêu cầu đến authoriative name server. Khi name sever A gửi một truy vấn tương tác tới name server B, nếu name server B không có ánh xạ được yêu cầu, nó sẽ gửi cho A thông điệp trả lời chứa địa chỉ IP của name server kế tiếp trên chuỗi, giả sử là name sever C. Sau đó name server A trực tiếp gửi thông điệp yêu cầu tới name server C.



Các truy vấn trong dãy truy vấn liên tiếp có thể là tương tác hoặc đệ quy như minh hoạ trên hình 5. Thông thường tất cả các truy vấn là đệ quy - ngoại trừ truy vấn từ local name server tới root name server, truy vấn tới root name server thường là tương tác (bởi vì root name server phải xử lý một lượng lớn các yêu cầu nên cần làm giảm số lượng truy vấn tới root name server).

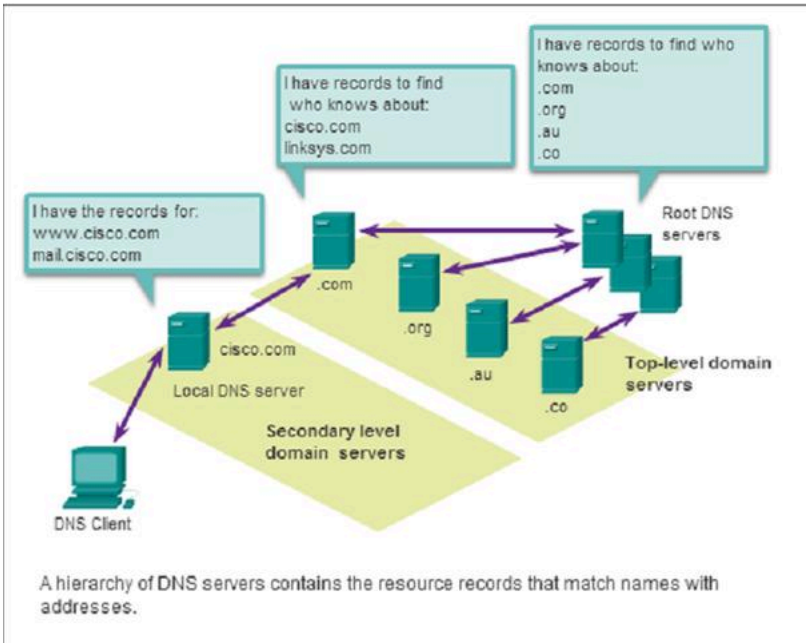
DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS

DNS của máy tính nào đó, bên cạnh việc gửi tiếp thông điệp, name server sẽ lưu ánh xạ này vào bộ nhớ cục bộ (ổ đĩa cứng hay RAM). Với ánh xạ tên máy - địa chỉ IP được lưu trữ, nếu có một truy vấn khác yêu cầu địa chỉ IP của cùng tên máy mà name server vừa lưu trữ, nameserver sẽ xác định được địa chỉ áp mong muốn, ngay cả khi nó không là authoritiative name server cho máy tính đó. Để khắc phục tình trạng bị lạc hậu, thông tin được lưu trữ tạm thời sẽ bị xoá bỏ sau một khoảng thời gian (thường là hai ngày).



Hình 5 Các truy vấn đệ quy và tương tác

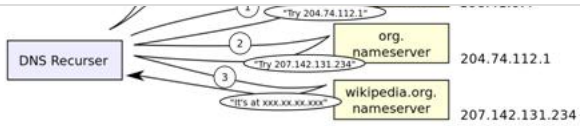
[h=2]2.1. Mô hình phân cấp các server DNS (slide CCNA cisco)[/h]**[FONT=&quot][/FONT]**



Hình 6 Mô hình phân cấp các server DNS

Root: có 13 server trên toàn thế giới (ở đó có thông tin về các top-level domain server).
- Top-level domain server: là các server chứa các thông tin cho các tên miền cụ thể như .com, .org, .au, .co,…
Ví dụ 1 vài top-level domain:
+ .au: đuôi của nước Australia (Úc).
+ .jp: đuôi của nước Japan (Nhật).
+ .co: đuôi của nước Colombia.
- Secondary level domain server: là các server chứa cụ thể thông tin đầy đủ về các tên miền đặc biệt mà nó lưu trữ (có thể là local name server hoặc authoriative name server).

DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS



[h=2]2.2. Ví dụ về truy vấn tên miền wikipedia.org[/h] [h=1]3. Bản ghi DNS.[/h]Name server cũng triển khai cơ sở dữ liệu phân tán DNS, ghi lại các bản ghi tài nguyên (resource record) cho các ánh xạ Tên máy 1 Địa chỉ IP. Mỗi thông điệp trả lời DNS chứa một hay nhiều bản ghi tài nguyên. Trong phần này chúng ta sẽ nói qua về bản ghi tài nguyên và thông điệp DNS. Về chi tiết, bạn có thể xem trong DNS RFC [RFC l034, RFC l035].

Bản ghi tài nguyên gồm 4 trường sau:

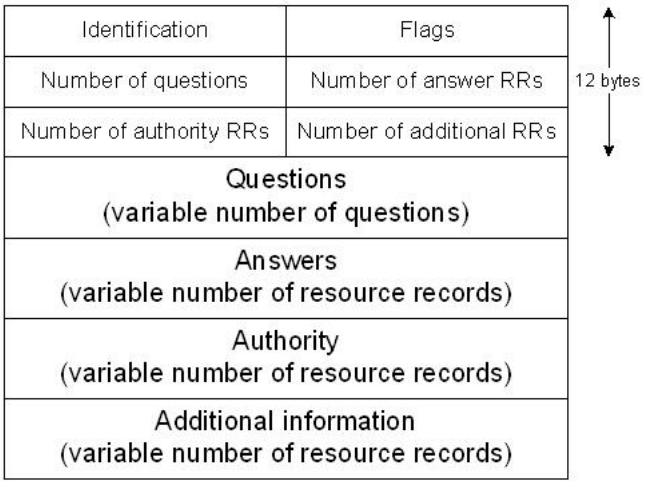
(Name, Value, Type, TTL)

TTL là thời gian tồn tại của bản ghi tài nguyên, dùng để xác định thời điểm có thể xoá bản ghi tài nguyên khỏi bộ nhớ lưu trữ. Trong các bản ghi ví dụ dưới đây, chúng ta bỏ qua trường TTL. Ý nghĩa của trường Name và Value phụ thuộc vào trường Type:

- Nếu Type = A (Address record) thì Name là tên máy và Value là địa chỉ IP của máy đó. Bản ghi kiểu A là ánh xạ Tên máy - Địa chỉ IP chuẩn. Ví dụ, (relay1.bar.foo.com, 145.37.93.126, A) là một bản ghi Type A.
- Nếu Type = NS thì Name là một miền (như là foo.com) và Value là tên máy của authoriative name server của các máy tính trong miền đó. Bản ghi này thường được sử dụng để gửi tiếp các truy vấn DNS. Ví dụ 1 bản ghi Type NS: (foo.com, dns.foo.com, NS)
- Nếu Type = CNAME thì Value là tên đầy đủ của máy có tên bí danh đặt trong Name. Bản ghi kiểu này cho phép xác định tên đầy đủ của một máy tính từ tên bí danh. Ví dụ một bản ghi CNAME: (foo.com, relay1 .bar.foo.com, CNAME).
- Nếu Type = MX thì Value là tên máy của mail server có tên bí danh đặt trong Name. Ví dụ, bản ghi kiểu MX (foo.com, mail.bar.foo.com, MX). Bản ghi MN cho phép mail server có tên bí danh đơn giản.
- Nếu Type = AAAA (Ipv6 address record) thì Name là tên máy, Value là địa chỉ Ipv6 của máy đó.

Ngoài ra còn nhiều loại bản ghi DNS khác như AFSDB (AFS database record), APL (Address Prefix List), CAA (Certification Authority Authorization), CDNSKEY (Child DNSKEY), CDS (Child DS), CERT (Certificate record), DHCID (DHCP identifier),… Nếu một name server là authoritiative name server cho một máy tính nào đó thì name server sẽ chứa bản ghi kiểu A của máy tính đó (ngay cả nếu name server đó không là authoritiative name server thì có thể nó chứa bản ghi kiểu A trong bộ nhớ cache của nó). Nếu name server không là authoritiative name server của máy tính được hỏi thì nó sẽ chứa một bản ghi kiểu NS cho miền của máy tính này, và nó cũng có một bản ghi kiểu A xác định địa chỉ IP của name server của miền này đặt trong trường Value của bản ghi NS. Ví dụ, root name server không là authoritiative name server cho máy tính gai.cs.umass.edu, root server sẽ có một bản ghi cho miền chứa cs.umass.edu ví dụ (umass.edu, dns.umass.edu, NS). Root server đó cũng có một bản ghi kiểu A cho phép xác định địa chỉ IP của name server dns.umass.edu, chẳng hạn (dns.umass.edu, 128.119.40.111, A)

[h=1]4. Thông điệp DNS:[/h]Có hai hoại thông điệp DNS: thông điệp yêu cầu và thông điệp trả lời. Cả hai kiểu thông điệp này có chung khuôn dạng minh hoạ trên hình 7.



Hình 7 Khuôn dạng thông điệp DNS

Ý nghĩa các trường trong thông điệp như sau:

- 12 byte đầu tiên là phần tiêu đề. Phần tiêu đề có một số trường. Trường đầu tiên là một định danh 16 bit cho mỗi thông điệp yêu cầu. 16 bít định đanh này được ghi lại vào thông điệp trả lời, cho phép client xác định được đấy là câu trả lời cho thông điệp yêu cầu nào. Có nhiều cờ trong trường cờ (mối cờ ứng với một bit).Cờ truy vấn (query/reply flag) xác định thông điệp là yêu cầu (0) hay là trả lời (1). Cờ authoritiative được đặt trong thông điệp trả lời khi name server 1à authoriative name server của tên máy tính cần xác định địa chỉ IP. Cờ mong muốn đệ quy (recursive-desired query) được đặt khi client (máy tính hay name server) mong muốn name server thực hiện truy vấn đệ quy khi nó không có bản ghi đó. Cờ chấp nhận đệ quy (recursion-available flag) được đặt trong thông điệp trả lời nếu name server đó hỗ trợ đệ quy. Trong phần tiêu đề cũng có 4 trường số lượng, các trường này xác định số lượng các bản ghi trong 4 phần dữ liệu sau phần tiêu đề
- Phần câu hỏi (Question session) chứa thông tin về câu hỏi được tạo ra. Nó bao gồm (1) trường tên chứa tên đang được hỏi và

DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS

đó. Chú ý rằng mỗi bản ghi tài nguyên có 4 trường: Type (A, NS, CNAME, MX,…), Name, Value, TTL. Thông điệp trả lời có thể có nhiều bản ghi tài nguyên vì tên máy tính có thể ứng với nhiều địa chỉ IP.
- Mục thẩm quyền (authonty section) chứa các bản ghi của các authoritative server.
- Mục phụ trợ (additional section) chứa các bản ghi "hữu ích" khác. Ví dụ trường trả lời trong thông điệp trả lời một truy vấn MX sẽ chứa tên đầy đủ của mail server có tên bí danh đặt ở trong Name. Phần phụ trợ có thể có một bản ghi kiểu A cung cấp địa chỉ IP cho chính mail server đó.
Các phần trên mô tả cách thức lấy dữ liệu trong cơ sở dữ liệu DNS. Vậy làm thế nào để đưa được dữ liệu vào cơ sở dữ liệu? Cho tới gần đây, nội dung của server DNS được cấu hình tĩnh, ví dụ, thông qua file cấu hình được người quản trị hệ thống tạo ra Gần đây, lựa chọn UPDATE được đưa vào giao thức DNS cho phép dữ liệu được tự động thêm vào hay xoá bỏ khỏi cơ sở dữ liệu thông qua thông điệp DNS. RFC 2136 đặc tả quá trình cập nhật động của DNS. Có thể xem thêm chi tiết trong [DNSNET 1999] hay [BIND 1999]
[h=1]5. Cách sử dụng DNS[/h]Do các DNS có tốc độ biên dịch khác nhau, có thể nhanh hoặc có thể chậm, do đó người sử dụng có thể chọn DNS server để sử dụng cho riêng mình. Có các cách chọn lựa cho người sử dụng. Sử dụng DNS mặc định của nhà cung cấp dịch vụ (internet), trường hợp này người sử dụng không cần điền địa chỉ DNS vào network connections trong máy của mình. Sử dụng DNS server khác (miễn phí hoặc trả phí) thì phải điền địa chỉ DNS server vào network connections. Địa chỉ DNS server cũng là 4 nhóm số cách nhau bởi các dấu chấm.
[h=1]Nguyên tắc làm việc của DNS[/h]- Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server riêng của mình, gồm các máy bên trong phần riêng của mỗi nhà cung cấp dịch vụ đó trong Internet. Tức là, nếu một trình duyệt tìm kiếm địa chỉ của một website thì DNS server phân giải tên website này phải là DNS server của chính tổ chức quản lý website đó chứ không phải là của một tổ chức (nhà cung cấp dịch vụ) nào khác.
- INTERNIC (Internet Network Information Center) chịu trách nhiệm theo dõi các tên miền và các DNS server tương ứng. INTERNIC là một tổ chức được thành lập bởi NFS (National Science Foundation), AT&T và Network Solution, chịu trách nhiệm đăng ký các tên miền của Internet. INTERNIC chỉ có nhiệm vụ quản lý tất cả các DNS server trên Internet chứ không có nhiệm vụ phân giải tên cho từng địa chỉ.
- DNS có khả năng truy vấn các DNS server khác để có được 1 cái tên đã được phân giải. DNS server của mỗi tên miền thường có hai việc khác biệt. Thứ nhất, chịu trách nhiệm phân giải tên từ các máy bên trong miền về các địa chỉ Internet, cả bên trong lẫn bên ngoài miền nó quản lí. Thứ hai, chúng trả lời các DNS server bên ngoài đang cố gắng phân giải những cái tên bên trong miền nó quản lí.
- DNS server có khả năng ghi nhớ lại những tên vừa phân giải. Để dùng cho những yêu cầu phân giải lần sau. Số lượng những tên phân giải được lưu lại tùy thuộc vào quy mô của từng DNS.
[h=1]Cú pháp tên miền[/h]http://en.wikipedia.org/wiki/Domain_Name_System

Có thể xem chi tiết mô tả trong RFC 1035, RFC 1123, RFC 2181. Một tên miền bao gồm 1 hoặc nhiều phần, về mặt kĩ thuật gọi là nhãn, được quy ước nối, và giới hạn bởi các dấu chấm, ví dụ như .com.
- Nhãn ngoài cùng bên phải chuyển tải top-level domain; ví dụ như tên miền www.example.com thuộc về top-level domain *com.*
- Phân cấp của tên miền theo thứ tự từ phải sang trái; mỗi nhãn bên trái chỉ định 1 phân cấp nhỏ hơn, hoặc một tên miền phụ của miền bên phải. Ví dụ: nhãn *example* chỉ định một tên miền phụ của tên miền *com*, và *www* là một tên miền phụ của *example.com.* Cây phân cấp này có thể lên tới 127 cấp độ (level).
- Mỗi nhãn có thể chứa lên đến 63 ký tự. Các tên miền đầy đủ không được vượt quá chiều dài của 253 kí tự. Trong biểu diễn nhị phân bên trong của DNS chiều dài tối đa đòi hỏi lưu trữ bằng 255 octet, vì nó cũng lưu độ dài của tên.
- Về mặt kĩ thuật thì tên DNS có thể bao gồm bất kì kí tự nào trong 1 octet, tuy nhiên, người ta chỉ cho phép tên miền ở DNS root zone, và ở hầu hết các tên miền phụ khác được biểu diễn bằng định dạng và kí tự sử dụng bộ kí tự ASCII (bao gồm các kí tự từ a-z, A-Z, 0-9, và dấu gạch nối). Điều luật này được biết đến với tên gọi điều luật LDH (letters, digits, hyphen). Nhãn không thể được bắt đầu hoặc kết thúc bằng 1 dấu gạch nối. Ngoài ra top-level domain không được toàn là số.
- Một hostname là một tên miền mà có thể được liên kết với các địa chỉ IP. Ví dụ, các tên miền *www.example.com* và *example.com* cũng là các hostname, trong khi đó *com* thì không phải.
[h=1]Authoritative name server[/h]http://en.wikipedia.org/wiki/Domain_Name_System

- Một máy chủ tên có thẩm quyền là một máy chủ tên cho câu trả lời đã được cấu hình bởi một nguồn nguyên bản, ví dụ, các quản trị viên miền hoặc bằng phương pháp DNS động, trái ngược với câu trả lời rằng đã thu được thông qua một truy vấn DNS thường xuyên đến một máy chủ tên khác. Một máy chủ tên có thẩm quyền chỉ chỉ trả về câu trả lời cho những thắc mắc về tên miền đã được cấu hình cụ thể bởi người quản trị.
- Nói cách khác, một máy chủ tên có thẩm quyền cho phép các máy chủ tên đệ quy biết dữ liệu DNS (IPv4, IPv6, một danh sách các máy chủ thư đến - incoming mail servers,…) mà một hostname nhất định có (chẳng hạn như "www.example.com"). Ví dụ, máy chủ tên có thẩm quyền của "example.com" cho các máy chủ tên đệ quy biết rằng "www.example.com" có địa chỉ IP IPv4 là 192.0.43.10.
- Một máy chủ tên có thẩm quyền hoặc có thể là một *master server* (server chính) hoặc một *slave server* (server phụ). Một master server là một server lưu trữ bản gốc (*master*) của tất cả các bản ghi vùng. Một slave server sử dụng một cơ chế tự động cập nhật của giao thức DNS trong giao tiếp với master server của nó để duy trì một bản sao giống hệt nhau của các bản ghi của

DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS

server đó phải được lưu trữ trong các parent zone và trong chính các server đó (để tự tham chiếu).
- Khi tên miền được đăng ký, cài đặt của chúng tại domain registry (đăng ký tên miền) của một top-level domain đòi hỏi cần phải có 1 name server chính và ít nhất 1 name server phụ. Việc đòi hỏi cần phải có nhiều name server nhằm mục đích dự phòng khi 1 name server không hoạt động được hoặc không truy cập được.
- Trong bản tin trả lời có chỉ ra server có thẩm quyền hay không, bằng cách thiết lập một cờ (một bit cấu trúc giao thức), được gọi là bit trả lời thẩm quyền (AA - *Authoritative Answer*) trong phản hồi của server có thẩm quyền. Cờ này thường được sao chép lại một cách nổi bật trong đầu ra các công cụ truy vấn quản trị DNS (như *dig*) để chỉ ra rằng name server phản hồi là có thẩm quyền cho tên miền được hỏi.
[h=1]Recursive and caching name server (Server đệ quy và server tên đệm - server trả lời hộ)
[/h]http://en.wikipedia.org/wiki/Domain_Name_System

Về lý thuyết thì chỉ cần các máy chủ tên có thẩm quyền là đủ cho hoạt động của mạng Internet. Tuy nhiên, chỉ với sự vận hành của các máy chủ tên có thẩm quyền, tất cả các truy vấn DNS phải bắt đầu với các truy vấn đệ quy ở vùng root của hệ thống tên miền và mỗi hệ thống người dùng sẽ phải thực hiện các phần mềm giải quyết khả năng hoạt động đệ quy.
Để nâng cao hiệu quả, làm giảm lưu lượng DNS trên Internet, và tăng hiệu suất trong các ứng dụng của người dùng cuối, các hệ thống tên miền hỗ trợ các máy chủ DNS cache trong đó lưu trữ các kết quả truy vấn DNS cho một khoảng thời gian xác định trong cấu hình (time-to-live) của bản ghi tên miền. Thông thường, như các máy chủ DNS caching, còn được gọi là bộ nhớ cache DNS, cũng thực hiện các thuật toán đệ quy cần thiết để phân giải một tên được bắt đầu với các truy vấn thông qua DNS root tới các máy chủ tên có thẩm quyền của miền truy vấn. Với chức năng này được thực hiện trong name server, ứng dụng người dùng đạt được hiệu quả trong thiết kế và vận hành.
Ví dụ như, nếu một client muốn biết địa chỉ cho "www.example.com", nó sẽ gửi, đến một recursive caching name server, một yêu cầu DNS nêu "Tôi muốn các địa chỉ IPv4 cho 'www.example.com'. "Sau đó các máy chủ tên đệ quy sẽ truy vấn các máy chủ tên có thẩm quyền cho đến khi nó được một câu trả lời cho câu hỏi đó (hoặc trả lại một lỗi, nếu nó không thể có được một câu trả lời) - trong trường hợp này là 192.0.43.10.
Sự kết hợp của bộ nhớ đệm DNS và chức năng đệ quy trong một name server không bắt buộc; các chức năng có thể được thực hiện độc lập trong các server cho các mục đích đặc biệt.
Các nhà cung cấp dịch vụ Internet thường cung cấp các máy chủ tên đệ quy và bộ nhớ đệm cho khách hàng của họ. Ngoài ra, rất nhiều router mạng gia đình thực hiện cache DNS và recursors (đệ quy) để nâng cao hiệu suất trong mạng nội bộ.
[h=1]Sự phụ thuộc vòng tròn và bản ghi keo (Circular dependencies and glue records)[/h] Sẽ có 1 sự phụ thuộc vòng tròn lẫn nhau xảy ra bởi 1 lý do như sau.
Các name server được ủy quyền được xác định bởi tên, chứ không phải bằng địa chỉ IP. Điều này có nghĩa là một name server phân giải phải đưa ra một yêu cầu DNS để tìm ra địa chỉ IP của server mà nó đã được gọi. Nếu tên được đưa ra trong ủy quyền lại là một tên miền phụ của tên miền mà ủy quyền đang được cung cấp, thì sẽ có một sự phụ thuộc vòng tròn (vòng quanh).
Trong trường hợp này, name server cung cấp các ủy quyền cũng phải cung cấp một hoặc nhiều địa chỉ IP cho các name server

T **thuan06**

Re: DNS - Tư duy hoạt động DNS - Cơ chế hoạt động DNS - Một số thông tin chi tiết hơn về DNS

DNS cũng chạy ở TCP port 53 nữa nhé

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày.
Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan

DNS bao gồm một yêu cầu UDP đơn từ khách hàng tiếp theo là một bài trả lời UDP duy nhất từ server. Transmission Control Protocol (TCP) được sử dụng khi kích thước dữ liệu phản hồi vượt quá 512 byte, hoặc cho các tác vụ như chuyển vùng. Một số bộ phân giải sử dụng TCP cho tất cả các truy vấn.

Bài viết liên quan

DRMAC - tiêu chuẩn xác thực email ngăn chặn giả mạo tên miền
15/01/2024 · 0

Tin tặc Iran sử dụng back door DNS nhắm mục tiêu vào lĩnh vực năng lượng
08/09/2022 · 0

Lỗi khi sử dụng DNS spoof Kali Linux ?
24/08/2015 · 9

Máy chủ DNS của nhà cung cấp dịch vụ Internet Hàn Quốc bị tấn công
01/12/2014 · 1

Hỏi về DNS Server hoặc cấu hình VPS windows
16/04/2014 · 5

Cách Domain Name System (DNS) hoạt động
07/12/2013 · 12

WarGame
Thảo luận
Video

Thông kê - WhiteHat Forum