Chương 19: Domain Name System (DNS)

Giới thiệu: Trong chương này, ta sẽ thảo luận về Domain Name System (DNS), được dịch là Hệ thống phân giải tên cho Internet. DNS là một chương trình ứng dụng client/server, được dùng để hỗ trợ các chương trình ứng dụng khác. DNS có thể liên kết một tên miền trong lớp Application với địa chỉ IP trong lớp Network.

Mục tiêu

* Mô tả mục đích của DNS.
* Xác định khái niệm về miền và không gian miền.
* Mô tả sự phân phối của không gian tên và vùng xác định.
* Thảo luận về sử dụng của DNS trong Internet và mô tả ba loại miền: miền chung, miền quốc gia và miền nghịch đảo.
* Thảo luận về sự phân giải tên-địa chỉ và chỉ ra hai phương pháp phân phối: đệ quy và lặp lại.
* Chỉ ra định dạng của tin nhắn DNS và cách nén.
* Thảo luận DDNS and DNSSEC.

19.1 DNS LÀ CẦN THIẾT.

Để xác định một thực thế, giao thức TCP/IP sử dụng địa chỉ IP, cách duy nhất để xác định kết nối từ host tới Internet. Tuy nhiên, người ta thích sử dụng tên hơn là địa chỉ bằng những con số. Do vậy, chúng ta cần một hệ thống có thể liên kết một cái tên với một địa chỉ cũng như giữa một địa chỉ và một cái tên.

Trước đây, khi mà Internet vẫn còn chưa rộng rãi, việc liên kết này được sử dụng bằng một *host file.* Host file chỉ có 2 cột: tên và địa chỉ. Mỗi host có thể chứa host file trên ổ đĩa và cập nhật đều đặn từ một *master host file*. Khi một chương trình hoặc người dùng muốn truy cập, host sẽ dùng host file để tìm liên kết.

Tuy nhiên, ngày nay, điều này trở nên bất khả thi để có host file riêng lẻ trên mỗi host vì dung lượng quá lớn để chứa. Thêm vào đó, không thể cập nhật toàn bộ host files mỗi khi có thay đổi.

Một giải pháp đó là chứa toàn bộ host file trên duy nhất một máy tính và cho phép mỗi máy tính khác truy cập vô nguồn thông tin trung tâm này. Tuy nhiên, chúng ta biết rằng điều này sẽ tạo ra một mạng lưới giao thông cực lớn trên Internet.

Một giải pháp khác, cũng là phương pháp được dùng ngày nay, là chia lượng thông tin khổng lồ này thành các phần nhỏ hơn và chứa trên nhiều máy tính khác nhau. Với phương pháp này, host cần các liên kết có thể kết nối với máy tính gần nhất chứa dữ liệu cần thiết. Phương pháp này chính là **Domain Name System (DNS).** Trong chương này, đầu tiên chúng ta thảo luận về các khái niệm và ý tưởng tạo nên DNS. Sau đó ta mô tả giao thức DNS của chính nó.

Hình 19.1 chỉ ra cách TCP/IP dùng một máy khách DNS và một máy chủ DNS để liên kết tên với một địa chỉ; và cách liên kết ngược lại khá đơn giản.

Trong hình 19.1, một người dùng muốn sử dụng máy khách truyền tệp tin (File transfer client) để truy cập máy chủ truyền tệp tin (File transfer server) tương ứng trên một host điều khiển. Người dùng chỉ biết tên máy chủ là *forouzan.com*. Tuy nhiên, TCP/IP phù hợp cần địa chỉ IP của máy chủ để kết nối. 6 bước dưới để liên kết tên host với địa chỉ IP.

1. Người dùng chuyển tên host tới máy khách truyền tệp tin.
2. Máy khách truyền tệp tin chuyển tên host tới máy khách DNS.
3. Như đã biết, mỗi máy tính sẽ biết địa chỉ của một máy chủ DNS. Máy khách DNS gửi tin nhắn tới máy chủ DNS bằng truy vấn để cung cấp tên của máy chủ truyền tệp tin bằng địa chỉ IP của máy chủ DNS.
4. Máy chủ DNS phản hồi với địa chỉ IP của máy chủ truyền tệp tin.
5. Máy khách DNS chuyển địa chỉ IP tới máy chủ truyền tệp tin.
6. Máy khách truyền tệp tin có thể nhận địa chỉ IP để truy cập máy chủ truyền tện tin.

Lưu ý: Mục đích của truy cập Internet là tạo kết nối giữa máy chủ và máy khách truyền tệp tin, nhưng trước đó, một kết nối khác cần được tạo ra giữa máy chủ và máy khách DNS. Nói cách khác, ta cần hai kết nối, cái thứ nhất để liên kết tên với địa chỉ IP, cái thứ 2 để truyền tệp tin.

19.2 KHÔNG GIAN TÊN

Những cái tên được cấp cho các thiết bị phải được lựa chọn cẩn thận từ không gian tên (name space) với kiểm soát hoàn toàn việc gắn kết giữa những cái tên và địa chỉ IP. Nói cách khác, những cái tên phải là duy nhất bởi vì những địa chỉ là duy nhất. Một **Không gian tên** liên kết các địa chỉ với cái tên độc nhất đó có thể được tổ chức theo hai cách: Dạng phẳng và dạng phân cấp.

*Không gian tên dạng phẳng*

Trong Không gian tên phẳng, một cái tên được cấp cho một địa chỉ, một cái tên trong Không gian này là một chuỗi kí tự không cấu trúc. Những cái tên có thể hoặc không có phần chung. Bất lợi chính của Không gian tên phẳng là nó không thể sử dụng trong hệ thống lớn như Internet vì nó phải được là trung tâm điều khiển để tránh mơ hồ hoặc trùng.

*Không gian tên dạng phân cấp*

Trong Không gian tên phân cấp, mỗi cái tên được tạo thành từ nhiều phần. Phần đầu tiên có thể xác định đặc điểm tổ chức, phần thứ hai có thể xác định tên tổ chức, phần thứ ba có thể xác định các bộ phận của tổ chức đó, và cứ thế tương tự. Trong trường hợp này, có thể phân quyền quyền cấp phát và điều khiển những không gian tên. Quyền trung tâm có thể cấp cho phần tên mô tả đặc điểm tổ chức của và tên của tổ chức đó. Trách nhiệm của phần còn lại của cái tên là có thể cấp để tự tổ chức. Tổ chức có thể thêm vào hậu tố (hoặc tiền tố) của tên để xác định host và tài nguyên (resources). Sự quản lý tổ chức sẽ không nghiêm trọng hóa vấn đề tiền tố được chọn cho host sẽ lấy mất các phần còn lại của cách tổ chức, vì cho dù một phần của địa chỉ trùng nhau, nhưng toàn bộ địa chỉ vẫn khác biệt. Cho ví dụ, cho hai trường học và một công ty gọi một máy tính của họ là *kẻ thách thức* (challenger). Trường học thứ nhất vẫn được cấp cái tên bởi quyền trung tâm là *fhda.edu*, trường học thứ hai được cấp tên *berkeley.edu*, và công ty kia được cấp tên là *smart.com*. Khi mỗi tổ chức thêm cái tên *kẻ thách thức* vào tên họ đã được cấp sẵn, kết quả cuối cuối là ba phần phân biệt: *challenger.fhda.edu, challenger.berkeley.edu* và *challenger.smart.com*. Những cái tên là duy nhất mà không bắt buộc phải là trách nhiệm của quyền trung tâm. Quyền trung tâm chỉ điều khiển một phần của cái tên, không phải toàn bộ.

*Không gian tên miền (Domain Name Space)*

Để có một không gian tên kiểu phân cấp, một không gian tên miền được thiết kế ra. Trong thiết kế này, những cái tên được xác định bằng dạng cây ngược với gốc nằm ở đỉnh. Cái cây chỉ có thể có 128 cấp độ: cấp độ 0 (gốc), tới cấp độ 127. (Xem hình 19.2)

*Nhãn (Label)*

Mỗi nút (node) trên cây có một nhãn, là một chuỗi dài tối đa 63 kí tự. Nhãn của gốc là chuỗi rỗng. DNS yêu cầu là các nút con của một node phải có nhãn khác nhau, điều này đảm bảo sự độc nhất của tên miền.

*Tên miền (Domain Name)*

Mỗi nút trong cây có một tên miền. Một tên miền đầy đủ alf thứ tự các nhãn, phân biệt bởi dấu chấm (.). Tên miền luôn được đọc lên cho đến gốc. Nhãn cuối cùng sẽ là nhãn của gốc (trống). Điều này nghĩa là tên miền đầy đủ luôn kết thúc bằng một nhãn trống, đồng nghĩa với kí tự cuối cùng sẽ là dấu chấm vì chuỗi trống không có gì cả. Hình 19.3 chỉ ra một số tên miền

*Tên miền đầy đủ tiêu chuẩn (Fully Quanlified Domain Name – FQDN)*

Nếu một nhãn được kết thúc bởi một chuỗi trống, nó được gọi là Tên miền đầy đủ tiêu chuẩn. Một FQDN là một tên miền chứa toàn bộ tên của một host. Nó chứa tất cả nhãn, từ cái cụ thể nhất đến cái chung nhất, để xác định duy nhất tên host. Cho ví dụ, tên miền là FQDN của máy tính tên là *Kẻ thách thức* (challenger) được cài đặt bởi Trung tâm công nghệ cao (Advanced Technology Center – ATC) tại Trường De Anza. Một máy chủ DNS chỉ có thể nốt một FQDN tới một địa chỉ. Lưu ý rằng cái tên phải kết thúc bởi một chuỗi trống, nhưng không có nghĩa trống là không có gì, nhãn kết thúc với một dấu chấm (.).

Ví dụ: *challenger.atc.fhda.edu.*

*Tên miền tiêu chuẩn một phần (Partially Quanlified Domain Name – PQDN)*

Nếu một nhãn không kết thúc bởi một chuỗi trống, nó được gọi là tên miền tiêu chuẩn một phần. Một PQDN bắt đầu với một nút, nhưng không chạm tới gốc. Nó được dùng khi mà tên được chỉ ra là cùng thuộc chung vị trí với máy khách. Bộ phận giải quyết có thể cung cấp phần còn thiếu, được gọi là hậu tố, để tạo nên một FQDN. Cho ví dụ, nếu một người dùng tại vị trí *fhda.edu.* muốn lấy địa chỉ IP của máy tính *Kẻ thách thức* (challenger), họ có thể xác định một phần tên

Ví dụ: *challenger*

Máy khách DNS thêm hậu tố *atc.fhda.edu.* trước khi chuyển địa chỉ tới máy chủ DNS.

Máy khách DNS thông thường có thể giữ một danh sách các hậu tố. Sau đây có thể là danh sách các hậu tố của Trường De Anza. Hậu tố trống xác định không có gì. Hậu tố này được thêm vào khi người dùng xác định một FQDN.

Ví dụ: *atc.fhda.edu fhda.edu trống*

Hình 19.4 chỉ ra một vài FQDN và PQDN

*Miền (Domain)*

Một miền là một cây con của một không gian tên miền. Tên của miền là tên của nút trên đỉnh của cây con. Hình 19.5 chỉ ra một số miền. Lưu ý rằng một miền có thể tự chia thành các miền khác (hoặc miền con – subdomain)

Sự phân phối của không gian tên (Distribution of Name Space)

Thông tin được chứa trong không gian tên miền phải được lưu trữ. Tuy nhiên, không hề hiệu quả và đáng tin cậy nếu có một máy tính chứa một lượng thông tin khổng lồ như vậy. Không hiệu quả bởi vì phản hồi từ các yêu cầu từ mọi nơi trên thế giới đặt sức nặng lên hệ thống. Không đáng tin cậy bởi vì bất kì lỗi nào sẽ làm dữ liệu không thể truy cập được nữa.

*Phân cấp tên máy chủ (Hierarchy of Name Servers)*

Giải pháp tới những vấn đề này là phân phối thông tin lên nhiều máy tính gọi là các máy chủ DNS. Một cách để thực hiện là chia toàn bộ không gian ra nhiều miền dựa trên cấp độ thứ nhất. Nói cách khác, chúng ta cho gốc đứng một mình và tạo ra nhiều miền (domain – subtree) như là các nút cấp độ thứ nhất. Bởi vì miền được tạo bằng cách này có thể rất lớn, DNS cho phép các miền được chia tiếp thành các miền nhỏ hơn (miền con - subdomain). Mỗi máy chú có thể phản hồi với bất kể miền lớn hay nhỏ. Hay là, chúng ta có một phân cấp các máy chủ bằng cái cách mà chúng ta có phân cấp các cái tên.

*Vùng (Zone)*

Từ khi tên phân cấp tên miền hoàn thiện không thể chứa trên một máy chủ đơn lẻ, nó được chia ra nhiều máy chủ khác. Nơi mà một máy chủ phải hồi hoặc có quyền hành được gọi là một Vùng (zone). Chúng ta có thể xác định một vùng như là các phần tiếp theo của toàn bộ cây. Nếu máy chủ chấp nhận trách nhiệm cho một miền và không chia miền ra nhiều miền nhỏ hơn, miền và vùng sẽ đều ám chỉ cùng một thứ. Máy chủ tạo cơ sở dữ liệu là *zone file* và giữ toàn bộ thông tin cho mỗi nút dưới miền đó. Tuy nhiên, nếu một máy chủ chia những miền của nó thành miền con và các phần ủy nhiệm quyền hành của nó với các máy chú khác, miền và vùng ám chỉ những thứ khác nhau. Thông tin về các nút trong miền con được lưu trữ trong máy chủ tại cấp độ thấp hơn, với máy chủ gốc giữ một vài sắp xếp về quan hệ ở các máy chủ cấp độ thấp hơn. Tất nhiên máy chủ gốc vẫn có trách nhiệm: Nó vẫn phải có một vùng, nhưng thông tin chi tiết được lưu bởi những máy chủ cấp độ thấp hơn. (Xem hình 19.7)

Một máy chủ cũng có thể chia các phần của miền của nó và giao trách nhiệm nhưng vẫn giữ phần miền cho riêng nó. Trong trường hợp này, vùng của nó được tạo ra bởi thông tin chi tiết cho vùng của miền mà không được ủy quyền và tương quan với những phần được ủy quyền.

*Máy chủ gốc (Root Server)*

Một máy chủ gốc (Root server) là một máy chủ mà vùng của nó chứa toàn bộ cây. Một máy chủ gốc thường không chứa bất kì thông tin gì về các miền nhưng ủy quyền cho các máy chủ khác, giữ tương quan với các máy chủ đó. Có rất nhiều máy chủ gốc, mỗi trong số chúng bao quát toàn bộ không gian tên miền. Các máy chủ gốc được phân phối khắp thế giới.

*Máy chủ sơ cấp và máy chủ trung cấp (Primary and Secondary Servers)*

DNS xác định hai loại máy chủ: sơ cấp và trung cấp. Một máy chủ sơ cấp là một máy chủ chứa một tệp tin về vùng ủy quyền. Nó có trách nhiệm để tạo, duy trì và nâng cấp tệp tin vùng. Nó chứa tệp tin vùng trên bộ nhớ cục bộ.

Một máy chủ trung cấp là một máy chủ truyền thông tin đẩy đủ về một vùng từ máy chủ khác (sơ cấp hoặc trung cấp) và chứa tệp tin đó trên bộ nhớ cục bộ. Máy chủ trung cấp không tạo hay nâng cấp các tệp tin vùng. Nếu cần nâng cấp, nó sẽ được thực thi bởi máy chủ sơ cấp, sau đó chuyển phiên bản nâng cấp tới máy chủ trung cấp.

Máy chủ sơ cấp và trung cấp đều có quyền cho các vùng chúng phục vụ. Ý tưởng là không đặt máy chủ trung cấp ở các cấp độ đặc quyền thấp hơn nhưng tạo các dư các dữ liệu để mà khi máy chủ có vấn đề, những máy chủ khác vẫn có thể tiếp tục phục vụ các máy khách. Lưu ý rằng một máy chủ có thể là máy chủ sơ cấp cho một vùng cụ thể và là máy chủ trung cấp cho một vùng khác. Vì vậy, khi chúng ta nói về một máy chủ là sơ cấp hay trung cấp, cần cẩn thạn về vùng mà chúng ta đề cấp đó.

Một máy chủ sơ cấp tải toàn bộ thông tin từ bộ nhớ tệp tin; máy chủ trung cấp tải toàn bộ thông tin từ máy chủ sơ cấp. Khi máy chủ trung cấp tải thông tin từ máy chủ sơ cấp, nó được gọi là truyền dẫn vùng (zone transfer)

19.3 DNS TRONG INTERNET

DNS là một giao thức mà có thể được dùng trên nhiều nền tảng khác nhau. Trong internet, không gian tên miền (cây) được chia thành ba thành phần: miền chung, miền quốc gia, và miền nghịch đảo.

*Miền chung (Generic Domains)*

Những miền chung (Generic domains) xác dịnh các host đăng kí dựa trên những hành vi chung. Mỗi nút trên cây xác định một miền, là một chỉ số của cơ sở dữ liệu không gian tên miền (Xem hình 19.9)

Nhìn vào cái cây, ta thấy cấp độ đầu tiên trong phần miền chung cho phép 14 nhãn. Những nhãn này mô tả loại của các tổ chức được liệt kê trong bảng 19.1.

*Miền quốc gia (Country Domains)*

Những miền quốc gia (country domains) sử dụng hai kí tự viết tắt quốc gia đó (ví dụ: us cho United States – Hợp chủng quốc Hoa Kỳ). Những nhãn thứ hai có thể được tổ chức, hoặc cụ thể hơn, định danh của quốc gia. Ví dụ: Hợp chủng quốc Hoa Kỳ sử dụng tên viết tắt của các bang là một phần của Hoa Kỳ (ca.us)

Hình 19.10 chỉ ra phần miền quốc gia. Địa chủ anza.cup.ca.us có thể được dịch thanh Trường De Anza ở Cupertino của bang California của Hợp chủng quốc Hoa Kỳ. (De Anza College in Cupertino in California in the United States).

*Miền nghịch đảo (Inverse Domain)*

Miền nghịch đảo được sử dụng để liên kết địa chỉ với cái tên. Điều này có thể xảy ra, ví dụ, khi một máy chủ nhận yêu cầu từ một máy khách thực hiện tác vụ. Mặc dù máy chủ có một tệp tin chứa danh sách các máy khách ủy quyền, chỉ có địa chỉ IP của máy khách được liệt kê. Máy chủ hỏi để giải quyết và gửi một truy vấn tới máy chủ DNS để liên kết địa chỉ với tên và xác thực máy khách có nằm trong danh sách ủy quyền.

Loại của truy vấn này được gọi là một truy vấn nghịch đảo hoặc con trỏ (inverse or pointer – PTR). Để chấp nhận một truy vấn con trỏ (pointer query), miền nghịch đảo được thêm vô không gian tên miền với nút ở cấp độ đầu tiên gọi là *arpa*. Cấp độ thứ hai cũng là một nút đơn tên *in-addr* (địa chỉ nghịch đảo). Và phần còn lại của miền xác định các địa chỉ IP.

Những máy chủ chứa vùng nghịch đảo cũng được phân cấp. Điều này nghĩa là phần netID của đại chỉ nên đạt cấp độ cao hơn phần netID con, và phần netID con nên có cấp độ cao hơn phần hostID. Bằng cách này, máy chủ phục vụ cả địa điểm được ở cấp đó cao hơn máy chủ phục vụ các vùng con. Cách cấu hình này làm cho miền nhìn có vẻ nghịch đảo lại khi so sánh với miền chung hay quốc gia. Để theo được quy ước đọc nhãn miền từ dưới lên trên, một địa chỉ IP như là 132.34.45.121 (phân lớp B với netID là 132.34) được đọc là 121.45.34.132.in-addr.arpa. Xem hình 19.11, mô tả cách cấu hình miền nghịch đảo.

*Công ty đăng ký (Registrar)*

Bằng cách nào những miền mới được thêm vô DNS? Điều này được thực hiện thông qua một công ty đăng ký (registrar), một công ty thương mại được công nhận bởi ICANN. Một công ty đăng ký đầu tiên xác minh rằng tên miền được yêu cầu là duy nhất và sau đó nhập vô cơ sở dữ liệu DNS. Tất nhiên phí phải được thanh toán.

19.4 SỰ PHÂN PHỐI (RESOLUTION)

Liên kết một tên với một địa chỉ hoặc một địa chỉ với một tên được gọi là phân phối tên-địa chỉ (name-address resolution).

*Nhà phân phối (Resolver)*

DNS được thiết kế là một ứng dụng máy chủ-khách (client-server application). Một host cần liên kết một địa chỉ với một tên hoặc một tên với một địa chỉ máy khách DNS được gọi là Nhà phân phối (resolver). Nhà phân phối truy cập máy chủ DNS gần nhất với một yêu cầu liên kết. Nếu máy chủ có thông tin, nó sẽ thỏa mãn được nhà phân phối, ngược lại, nó sẽ hướng dẫn nhà phân phối tới các máy chủ khác hoặc hỏi các máy chủ khác cung cấp thông tin.

Sau khi nhà phân phói nhận liên kết, nó diễn giải phản hồi để xem nếu đó đã được phân phối thực sự hay là một lỗi, và cuối cùng chuyển kết quả cho tiến trình yêu cầu nó.

*Liên kết tên và địa chỉ (Mapping Names to Addresses)*

Hầu hết thời gian, nhà phân phối đưa tên miền tới máy chủ và yêu cầu địa chỉ tương ứng. Trong trường hợp này, máy chủ kiểm tra miền chung hoặc miền quốc gia để tìm liên kết.

Nếu tên miền là từ phần miền chung, nhà phân phối nhận một tên miền như là *“chal.atc.fhda.edu”*. Truy vấn được gửi bởi nhà phân phối để tìm ra máy chủ DNS cục bộ cho sự phân phối này. Nếu máy chủ cục bộ không thể giải quyết truy vấn, nó dẫn nhà phân phối tới máy chủ khác hoặc trực tiếp hỏi các máy chủ khác.

Nếu tên miền là từ phần miền quốc gia, nhà phân phối nhận một tên miền như là “ch.fhda.cu.ca.us”. Phần công việc còn lại tương tự.

*Liên kết địa chỉ và tên (Mapping Addresses to Names)*

Một máy khách có thể gửi một địa chỉ IP tới máy chủ để liên kết một tên miền. Như đã đề cập trước đó, nó được gọi là truy vấn PTR. Để đáp lại truy vấn thế này, DNS sử dụng miền nghịch đảo. Tuy nhiên, trong yêu cầu, địa chỉ IP được đảo ngược và hai nhãn, *id-addr* và *arpa*, được nối để tạo ra một miền truy cập được bởi phần miền nghịch đảo. Cho ví dụ, nếu nhà phân phối nhận địa chỉ IP 132.34.45.121, nhà phân phối trước tiên đảo ngược địa chỉ và thêm hai nhãn đó vào trước khi gửi. Tên miền là *“121.45.34.132.in-addr.arpa”*, được nhận bởi DNS cục bộ và phân phối đi.

*Phân phối đệ quy (Recursive Resolution)*

Hình 19.12 chỉ ra phân phối đệ quy

Máy khách (nhà phân phối) có thể yêu cầu một câu trả lời đệ quy cho một tên máy chủ. Điều này nghĩa là nhà phân phối kì vọng máy chủ cung cấp câu trả lời cuối cùng. Nếu máy chủ có cho tên miền, nó kiểm tra cơ sở dữ liệu của nó để phản hồi. Nếu máy chủ không có, nó sẽ gửi yêu cầu tới một máy chủ khác (thường là máy chủ cha) và đợi phản hồi. Nếu máy chủ cha có cho được tên miền, máy chủ cha phản hồi và ngược lại, sẽ gửi truy vấn tiếp tục tới một máy chủ khác. Khi truy vấn cuối cùng được giải quyết, phản hồi được đưa ngược lại cho tới khi chạm tới yêu cầu của máy khách.

*Phân phối lặp lại (Iterative Resolution)*

Nếu máy khách không yêu cầu một câu trả lời đệ quy, liên kết có thể giải quyết một cách lặp lại.