Cẩm Nang
Toàn Diện về Hệ Thống Phân Giải Tên Miền (DNS)

Bộ tài liệu kỹ thuật

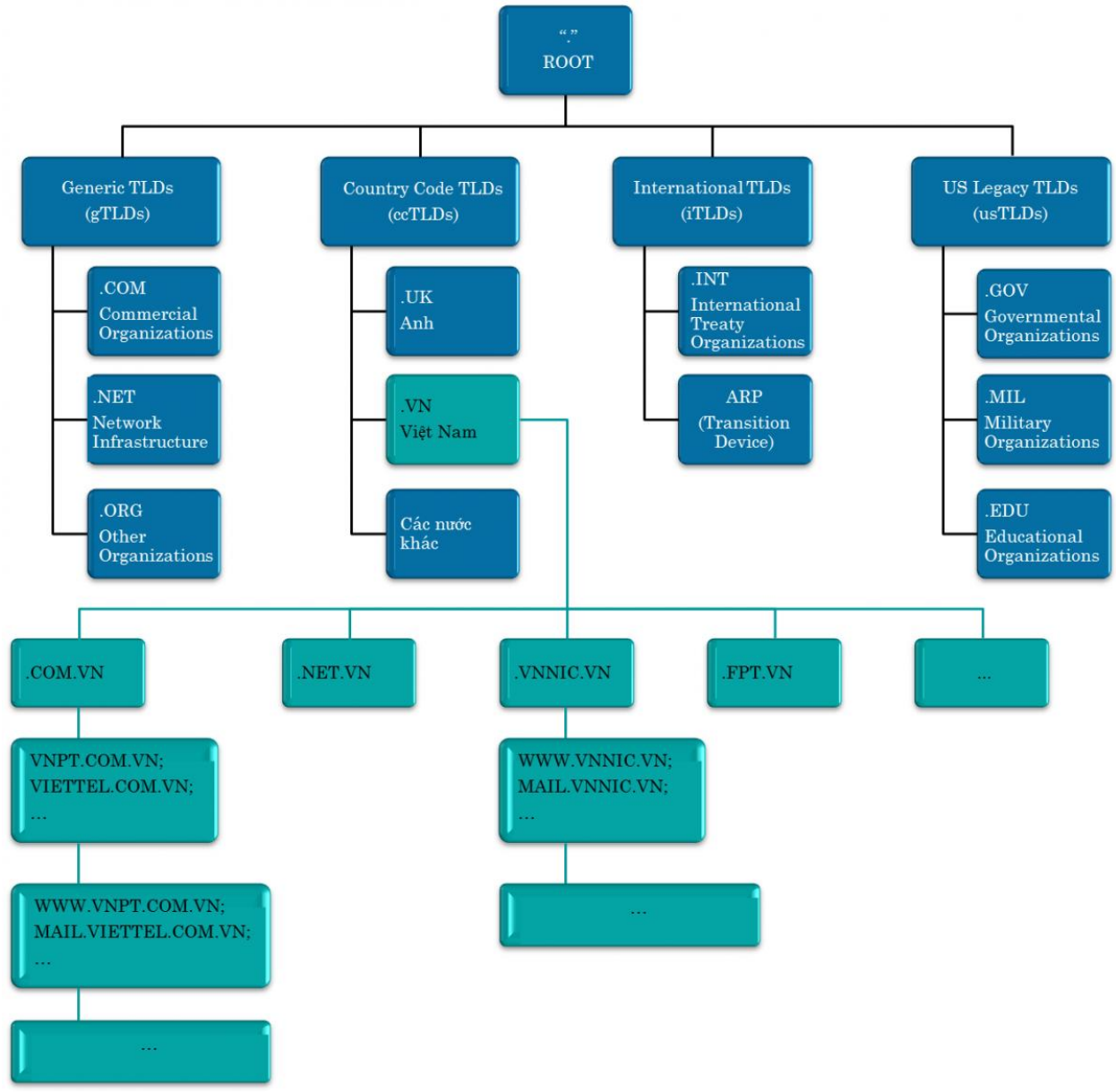
(Tài liệu lưu hành nội bộ)

Quý 3/2025

Contents

Chương 1: Giới thiệu Tổng quan về DNS - Nền tảng của Internet

1.1. DNS là gì? Định nghĩa và Vai trò Cốt lõi



Định nghĩa Kỹ thuật

Hệ thống Phân giải Tên miền, hay DNS (Domain Name System), là một hệ thống cơ sở dữ liệu phân cấp và phân tán trên toàn cầu, được phát minh vào năm 1984. Chức năng cốt lõi của nó là chuyển đổi, hay "phân giải", các tên miền mà con người có thể đọc và ghi nhớ (ví dụ: www.matbao.net) thành các địa chỉ IP (Internet Protocol) dạng số mà máy tính sử dụng để xác định và giao tiếp với nhau trên mạng (ví dụ:

103.21.150.210). Quá trình này cũng hoạt động theo chiều ngược lại, cho phép phân giải một địa chỉ IP trở lại tên miền tương ứng của nó, một quy trình được gọi là phân giải ngược.

Phép ẩn dụ "Danh bạ của Internet"
Để dễ hình dung, DNS có thể được coi như một cuốn danh bạ điện thoại khổng lồ và tự động của Internet. Trong thế giới thực, thay vì phải nhớ số điện thoại của mọi người, chúng ta chỉ cần nhớ tên của họ và tra cứu trong danh bạ. Tương tự, trên Internet, người dùng không cần phải nhớ hàng tỷ chuỗi số IP phức tạp và khó nhớ. Thay vào đó, họ chỉ cần nhập tên miền của trang web vào trình duyệt. DNS sẽ đóng vai trò là "người phiên dịch", tự động tra cứu và cung cấp "số điện thoại" (địa chỉ IP) chính xác để trình duyệt có thể thiết lập kết nối đến đúng máy chủ web.

Tầm quan trọng chiến lược
DNS không chỉ là một tiện ích mà là một thành phần nền tảng, không thể thiếu của cơ sở hạ tầng Internet toàn cầu. Nó không chỉ đơn giản hóa trải nghiệm người dùng mà còn là yếu tố then chốt quyết định tốc độ, độ tin cậy và khả năng truy cập của gần như mọi dịch vụ trực tuyến, từ việc duyệt web, gửi email, đến các ứng dụng đám mây và streaming. Sự phức tạp của hệ thống này nằm ở chỗ nó phải xử lý hàng tỷ yêu cầu phân giải từ khắp nơi trên thế giới tại bất kỳ thời điểm nào, đồng thời phải liên tục cập nhật hàng triệu thay đổi về tên miền và địa chỉ IP được thêm mới hoặc sửa đổi mỗi ngày.Vượt ra ngoài vai trò của một công cụ kỹ thuật đơn thuần, DNS thực chất là một lớp trừu tượng (abstraction layer) thiết yếu. Nó tạo ra một sự tách biệt mang tính chiến lược giữa danh tính logic của một dịch vụ (tên miền) và vị trí mạng của nó (địa chỉ IP). Ban đầu, các máy tính trên mạng ARPANET được xác định bằng địa chỉ số, một phương pháp nhanh chóng trở nên không thể quản lý khi mạng lưới phát triển. DNS ra đời để giải quyết vấn đề này, tạo ra một hệ thống định danh thân thiện với con người. Sự tách biệt này mang lại sự linh hoạt to lớn: một trang web có thể thay đổi nhà cung cấp dịch vụ lưu trữ (hosting), dẫn đến việc thay đổi hoàn toàn địa chỉ IP, nhưng tên miền của nó vẫn không đổi. Người dùng cuối không hề hay biết về sự thay đổi ở tầng hạ tầng này. Chính lớp trừu tượng này là nền tảng cho các công nghệ hiện đại như Mạng phân phối nội dung (CDN), cân bằng tải (load balancing), và chuyển đổi dự phòng (failover), tất cả đều hoạt động bằng cách thay đổi động các bản ghi DNS để hướng người dùng đến máy chủ tối ưu nhất mà không cần thay đổi tên miền họ đang truy cập. Do đó, DNS không chỉ là một "danh bạ" tĩnh mà còn là một "bộ điều phối giao thông" động và thông minh của Internet.

1.2. Phân biệt Địa chỉ IP (IPv4 và IPv6)

Địa chỉ IP là định danh duy nhất được gán cho mỗi thiết bị trên mạng để xác định vị trí và cho phép giao tiếp. Hiện có hai phiên bản chính đang được sử dụng song song.

- **IPv4 (Internet Protocol version 4):** Đây là phiên bản địa chỉ IP được sử dụng rộng rãi nhất. Nó sử dụng một không gian địa chỉ 32-bit, được biểu diễn dưới dạng bốn nhóm số thập phân, mỗi nhóm cách nhau bởi một dấu chấm (ví dụ: 203.113.131.1).
- **IPv6 (Internet Protocol version 6):** Là phiên bản mới hơn, được phát triển để giải quyết vấn đề cạn kiệt không gian địa chỉ của IPv4. IPv6 sử dụng một không gian địa chỉ 128-bit, cung cấp một số lượng địa chỉ gần như vô hạn. Nó được biểu diễn bằng các chuỗi số thập lục phân (hexadecimal) cách nhau bởi dấu hai chấm (ví dụ: 2001:4860:4860::8888).

1.3. Public DNS và Private DNS: Các Trường hợp Sử dụng

- Các máy chủ DNS có thể được phân loại dựa trên phạm vi truy cập của chúng: công cộng hoặc riêng tư.**Public DNS (DNS Công cộng):** Là các máy chủ DNS được thiết kế để có thể truy cập được trên Internet công cộng. Chúng được cung cấp bởi các tổ chức lớn như Google, Cloudflare, hoặc bởi chính các Nhà cung cấp Dịch vụ Internet (ISP). Mục đích của chúng là phục vụ các yêu cầu phân giải tên miền từ bất kỳ người dùng nào trên toàn cầu, giúp họ truy cập vào các trang web và dịch vụ trực tuyến.
- **Private DNS (DNS Riêng tư):** Còn được gọi là DNS nội bộ, được sử dụng trong các mạng cục bộ (intranet) của doanh nghiệp, trường học hoặc tổ chức, và thường được bảo vệ phía sau tường lửa. Chức năng chính của Private DNS là cho phép các máy tính và thiết bị trong mạng nội bộ có thể nhận dạng và giao tiếp với nhau bằng tên (ví dụ: mayin-ketoan) thay vì phải sử dụng địa chỉ IP nội bộ (ví dụ: 192.168.1.50). Người dùng từ bên ngoài Internet công cộng không được phép truy cập trực tiếp vào các máy chủ này.

Chương 2: Kiến trúc Phân cấp của Hệ thống Tên miền

Kiến trúc của DNS là một trong những yếu tố then chốt tạo nên sự thành công của nó. Thay vì một cơ sở dữ liệu tập trung, dễ bị quá tải và trở thành điểm lỗi duy nhất, DNS được thiết kế theo một cấu trúc cây phân cấp, phân tán trên toàn cầu.

2.1. Không gian Tên miền (Domain Name Space): Cấu trúc Cây Phân cấp

- Không gian tên miền của DNS được tổ chức theo một cấu trúc cây logic, bắt đầu từ một nút gốc (root) duy nhất. Mỗi nút trên cây đại diện cho một tên miền và có một nhãn (label) riêng. Các nút này chứa các bản ghi tài nguyên (Resource Records - RR), là những mẩu thông tin liên quan đến tên miền đó. Toàn bộ hệ thống có thể hỗ trợ tới 127 cấp độ phân cấp, mặc dù trong thực tế hiếm khi sử dụng đến mức đó.**Root Level (Tầng Gốc):** Đây là tầng cao nhất trong hệ thống, thường được biểu thị bằng một dấu chấm (.) ở cuối một tên miền đầy đủ (ví dụ: www.example.com.). Tầng này chứa các máy chủ DNS gốc (Root Servers), vốn là điểm khởi đầu cho mọi quá trình truy vấn phân giải tên miền.

2.2. Các Cấp Tên miền

Từ tầng gốc, không gian tên miền được chia thành các cấp khác nhau, tạo thành một hệ thống có tổ chức và dễ quản lý.

- **Top-Level Domain (TLD - Tên miền Cấp cao nhất):** Đây là phần cuối cùng của một tên miền, nằm ngay sau dấu chấm cuối cùng (ví dụ: .com, .org, .vn). Các TLD nằm ngay dưới tầng gốc và được quản lý bởi các máy chủ TLD chuyên biệt. TLD được chia thành hai loại chính:
    - **gTLD (generic TLDs):** Các TLD chung, không gắn với một quốc gia cụ thể. Các ví dụ kinh điển bao gồm .com (thương mại), .org (tổ chức), .net (mạng lưới), .edu (giáo dục). Gần đây, nhiều gTLD mới đã được giới thiệu như .app, .blog, .guru.
    - **ccTLD (country-code TLDs):** Các TLD được gán cho các quốc gia hoặc vùng lãnh thổ cụ

thể, bao gồm hai chữ cái, chẳng hạn như .vn cho Việt Nam, .us cho Hoa Kỳ, .uk cho Vương quốc Anh, và .jp cho Nhật Bản.

- **Second-Level Domain (SLD - Tên miền Cấp hai):** Là phần nằm ngay trước TLD, thường là tên định danh chính của một thương hiệu, tổ chức hoặc trang web. Ví dụ, trong google.com, google chính là SLD.
- **Subdomain (Tên miền phụ):** Là phần nằm trước SLD, được sử dụng để tạo ra một cấu trúc phân cấp sâu hơn cho trang web hoặc để phân chia các dịch vụ khác nhau. Ví dụ, trong blog.google.com, blog là một tên miền phụ của google.com.

Cấu trúc phân cấp này là một giải pháp xuất sắc cho vấn đề về quy mô và quản lý. Nếu toàn bộ thông tin tên miền được lưu trữ trên một máy chủ duy nhất, nó sẽ trở thành một điểm lỗi chí mạng (single point of failure) và một nút thắt cổ chai về hiệu suất không thể vượt qua. Kiến trúc phân cấp giải quyết vấn đề này thông qua cơ chế
ủy quyền (delegation). Máy chủ gốc không cần biết địa chỉ IP của www.google.com; nó chỉ cần biết máy chủ nào chịu trách nhiệm quản lý toàn bộ vùng .com. Tương tự, máy chủ của vùng
.com không cần biết thông tin chi tiết của tất cả các máy chủ thuộc Google; nó chỉ cần biết máy chủ nào có thẩm quyền cho vùng google.com. Sự ủy quyền này tạo ra một hệ thống có khả năng mở rộng gần như vô hạn và khả năng phục hồi cao. Việc quản lý được phân chia cho hàng ngàn tổ chức trên khắp thế giới, từ ICANN quản lý gốc, các nhà đăng ký quốc gia quản lý ccTLD, cho đến các chủ sở hữu tên miền tự quản lý vùng của mình. Đây là một ví dụ kinh điển về một hệ thống phân tán hoạt động hiệu quả trên quy mô toàn cầu.

2.3. Cú pháp và Các Khái niệm Liên quan

- **Fully Qualified Domain Name (FQDN - Tên miền Đầy đủ):** Là địa chỉ đầy đủ và duy nhất của một tài nguyên trên Internet. Một FQDN bao gồm tất cả các nhãn từ tên máy chủ, tên miền phụ (nếu có), SLD, TLD, và kết thúc bằng dấu chấm của tầng gốc (mặc dù dấu chấm cuối cùng này thường được các trình duyệt ẩn đi). Ví dụ, www.example.com. là một FQDN.
- **Internationalized Domain Names (IDN - Tên miền Quốc tế hóa):** Do sự giới hạn ban đầu của bộ ký tự ASCII, ICANN đã cho phép thiết lập hệ thống IDNA (Internationalized Domain Names in Applications). Hệ thống này cho phép sử dụng các ký tự Unicode, bao gồm cả các ngôn ngữ có dấu như tiếng Việt, trong tên miền. Ví dụ: http://TênMiềnTiếngViệt.vn.

Chương 3: Quy trình Phân giải Tên miền - Hành trình của một Truy vấn

Khi một người dùng nhập tên miền vào trình duyệt, một chuỗi các bước phức tạp nhưng diễn ra cực nhanh được thực hiện ở phía sau để tìm ra địa chỉ IP tương ứng. Quá trình này được gọi là phân giải DNS và có sự tham gia của nhiều loại máy chủ khác nhau.

3.1. Các Thành phần Chính trong Chuỗi Phân giải

- Quá trình phân giải DNS điển hình liên quan đến bốn loại máy chủ chính, mỗi loại có một vai trò

riêng biệt.**DNS Recursor (hoặc Recursive Resolver):** Đây là máy chủ đầu tiên nhận yêu cầu từ máy tính của người dùng (máy khách). Nó thường được vận hành bởi các Nhà cung cấp Dịch vụ Internet (ISP) hoặc các dịch vụ DNS công cộng (như Google DNS, Cloudflare DNS). DNS Recursor hoạt động như một "thủ thư" cần mẫn; nó chịu trách nhiệm thực hiện toàn bộ quá trình truy vấn, liên hệ với các máy chủ khác để tìm ra câu trả lời cuối cùng và trả về cho máy khách.

- **Root Name Server (Máy chủ Tên miền Gốc):** Đây là điểm khởi đầu của quá trình tra cứu. Trên toàn thế giới có 13 cụm máy chủ gốc logic, được quản lý bởi các tổ chức khác nhau. Các máy chủ này không biết địa chỉ IP của google.com, nhưng chúng biết địa chỉ của các máy chủ TLD chịu trách nhiệm cho vùng .com. Về cơ bản, chúng đóng vai trò là "bảng chỉ dẫn" cấp cao nhất.
- **TLD Name Server (Máy chủ Tên miền Cấp cao nhất):** Mỗi Tên miền Cấp cao nhất (như .com, .org, .vn) có một tập hợp các máy chủ TLD riêng. Các máy chủ này quản lý thông tin cho TLD đó. Khi được hỏi về google.com, máy chủ TLD của .com sẽ không biết địa chỉ IP cuối cùng, nhưng nó sẽ biết địa chỉ của các máy chủ có thẩm quyền cho tên miền google.com.
- **Authoritative Name Server (Máy chủ Tên miền có Thẩm quyền):** Đây là điểm đến cuối cùng của chuỗi truy vấn và là "nguồn sự thật" cho một tên miền cụ thể. Máy chủ này được quản lý bởi chủ sở hữu tên miền (hoặc nhà cung cấp dịch vụ của họ) và chứa thông tin chính thức, bao gồm các bản ghi DNS (như bản ghi A chứa địa chỉ IP). Nó sẽ cung cấp câu trả lời cuối cùng cho DNS Recursor.

3.2. Quy trình Phân giải Từng bước (Ví dụ: truy cập google.com)

Hành trình của một truy vấn DNS có thể được mô tả qua các bước sau :

1. **Người dùng gửi yêu cầu:** Người dùng nhập google.com vào trình duyệt. Máy tính (máy khách) tạo một truy vấn DNS và gửi nó đến DNS Recursor đã được cấu hình (thường là của ISP).
2. **Recursor kiểm tra bộ nhớ đệm (Cache):** Recursor đầu tiên sẽ kiểm tra bộ nhớ đệm của chính nó để xem liệu nó đã phân giải tên miền này gần đây chưa. Nếu có, nó sẽ trả lại địa chỉ IP ngay lập tức và quá trình kết thúc. Nếu không, nó sẽ chuyển sang bước tiếp theo.
3. **Recursor truy vấn Root Server:** Recursor gửi một truy vấn đến một trong các Root Name Server, hỏi "Tôi cần tìm google.com, ai quản lý vùng .com?".
4. **Root Server trả lời:** Root Server trả lời bằng một danh sách các địa chỉ IP của các TLD Name Server cho vùng .com.
5. **Recursor truy vấn TLD Server:** Recursor chọn một địa chỉ từ danh sách và gửi một truy vấn đến TLD Server của .com, hỏi "Tôi cần tìm google.com, ai là máy chủ có thẩm quyền cho tên miền này?".
6. **TLD Server trả lời:** TLD Server trả lời bằng địa chỉ IP của các Authoritative Name Server cho google.com.
7. **Recursor truy vấn Authoritative Server:** Recursor gửi truy vấn cuối cùng đến Authoritative Name Server của google.com, hỏi "Địa chỉ IP (bản ghi A) của google.com là gì?".
8. **Authoritative Server cung cấp câu trả lời:** Authoritative Server tìm trong cơ sở dữ liệu của nó và trả về địa chỉ IP chính xác của google.com cho Recursor.
9. **Recursor trả lời máy khách và lưu vào bộ đệm:** Recursor nhận được địa chỉ IP, chuyển nó cho trình duyệt của người dùng, và đồng thời lưu trữ (cache) thông tin này lại để tăng tốc cho các lần truy vấn trong tương lai.
10. **Trình duyệt kết nối:** Trình duyệt của người dùng giờ đã có địa chỉ IP và có thể thiết lập một kết nối HTTP/HTTPS trực tiếp đến máy chủ của Google để tải nội dung trang web.

3.3. Các Loại Truy vấn DNS: Đệ quy và Lặp

Quá trình phân giải phức tạp trên thực tế được tạo thành từ hai loại truy vấn cơ bản, mỗi loại phục vụ một mục đích khác nhau.

- **Truy vấn Đệ quy (Recursive Query):** Loại truy vấn này xảy ra giữa máy khách và DNS Recursor. Khi máy khách gửi một truy vấn đệ quy, nó yêu cầu Recursor phải chịu trách nhiệm hoàn toàn cho việc tìm ra câu trả lời cuối cùng. Máy khách chỉ mong đợi nhận lại địa chỉ IP hoặc một thông báo lỗi; nó không muốn bị "chỉ đường" đến các máy chủ khác.
- **Truy vấn Lặp (Iterative Query):** Loại truy vấn này xảy ra giữa DNS Recursor và các máy chủ Root, TLD, và Authoritative. Trong một truy vấn lặp, máy chủ được hỏi sẽ trả về câu trả lời tốt nhất mà nó có. Nếu nó không biết câu trả lời cuối cùng, nó sẽ cung cấp một tham chiếu đến máy chủ tiếp theo có thẩm quyền hơn. DNS Recursor sau đó phải "lặp lại" truy vấn của mình đến máy chủ mới được chỉ dẫn này.

DNS Recursor đóng một vai trò kép độc đáo: nó vừa là một *máy chủ* (server) đối với máy khách của người dùng, vừa là một *máy khách* (client) đối với các máy chủ DNS khác trong hệ thống phân cấp. Khi nhận yêu cầu từ trình duyệt, nó đóng vai trò là một máy chủ, hứa sẽ cung cấp một câu trả lời hoàn chỉnh (truy vấn đệ quy). Nhưng để thực hiện lời hứa đó, nó phải hành động như một máy khách, chủ động gửi các yêu cầu đến các máy chủ Root, TLD và Authoritative (truy vấn lặp). Vai trò trung tâm này làm cho Recursor trở thành một thành phần cực kỳ quan trọng đối với cả hiệu suất và bảo mật của toàn bộ hệ thống. Về mặt hiệu suất, bộ nhớ đệm (caching) của Recursor có thể đáp ứng phần lớn các truy vấn mà không cần lặp lại toàn bộ chuỗi phân giải, giúp giảm đáng kể độ trễ và tải cho các máy chủ cấp cao hơn. Về mặt bảo mật, vì Recursor là điểm tập trung các truy vấn từ nhiều người dùng, nó trở thành mục tiêu chính cho các cuộc tấn công như DNS Cache Poisoning. Nếu bộ đệm của một Recursor bị nhiễm độc, nó sẽ cung cấp thông tin sai lệch cho tất cả người dùng mà nó phục vụ, gây ra hậu quả trên diện rộng.Bảng dưới đây tóm tắt sự khác biệt chính giữa hai loại truy vấn:

Bảng 3.1: So sánh Truy vấn Đệ quy và Truy vấn Lặp

Đặc điểm	Truy vấn Đệ quy (Recursive Query)	Truy vấn Lặp (Iterative Query)
Bên tham gia	Máy khách (Client) và DNS Recursor	DNS Recursor và các máy chủ Root/TLD/Authoritative
Yêu cầu	Yêu cầu câu trả lời đầy đủ (địa chỉ IP cuối cùng) hoặc lỗi	Yêu cầu câu trả lời tốt nhất hiện có (thường là tham chiếu đến máy chủ khác)
Trách nhiệm phân giải	DNS Recursor chịu trách nhiệm hoàn thành toàn bộ quá trình	Máy chủ được hỏi chỉ cung cấp thông tin nó có, không tự tìm kiếm thêm
Luồng truy vấn	Một yêu cầu đi, một câu trả lời cuối cùng về	Một chuỗi các cặp yêu cầu-trả lời lặp đi lặp lại
Mục đích	Cung cấp địa chỉ IP cho ứng dụng của người dùng	Dẫn đường cho DNS Recursor đến được Authoritative Server

Chương 4: Các Loại Bản ghi DNS - Ngôn ngữ của Hệ thống Tên miền

Cơ sở dữ liệu của DNS được tạo thành từ các đơn vị thông tin được gọi là bản ghi tài nguyên (Resource Records - RR). Mỗi bản ghi này chứa một mẩu thông tin cụ thể về một tên miền. Việc hiểu rõ các loại bản ghi khác nhau là điều cần thiết để quản lý và cấu hình chính xác các dịch vụ liên quan đến tên miền.

4.1. Cấu trúc của một Bản ghi DNS (Resource Record - RR)

Mỗi bản ghi DNS, dù thuộc loại nào, đều tuân theo một cấu trúc chung bao gồm các trường thông tin chính sau :

- **Name (Tên):** Tên miền hoặc tên máy chủ mà bản ghi này áp dụng.
- **Type (Loại):** Xác định chức năng của bản ghi (ví dụ: A, MX, CNAME, v.v.).
- **TTL (Time To Live - Thời gian sống):** Một giá trị số, tính bằng giây, cho biết một máy chủ DNS khác (như DNS Recursor) được phép lưu trữ bản ghi này trong bộ nhớ đệm của nó trong bao lâu. Sau khi hết thời gian TTL, máy chủ phải thực hiện một truy vấn mới để lấy thông tin cập nhật.
- **Data/Value (Dữ liệu/Giá trị):** Đây là nội dung thực tế của bản ghi. Tùy thuộc vào loại bản ghi, trường này có thể chứa một địa chỉ IP, một tên miền khác, hoặc một chuỗi văn bản.

4.2. Bảng tra cứu các loại bản ghi DNS phổ biến

Mối quan hệ giữa các loại bản ghi DNS tạo thành một mạng lưới phụ thuộc phức tạp. Việc thay đổi một bản ghi có thể gây ra hiệu ứng lan truyền, ảnh hưởng đến nhiều dịch vụ khác nhau của một tên miền. Ví dụ, một tên miền (example.com) sử dụng bản ghi **NS** để chỉ định máy chủ có thẩm quyền. Trên máy chủ đó, bản ghi
A trỏ đến IP của máy chủ web. Tuy nhiên, bản ghi
MX cho email lại không trỏ đến IP mà trỏ đến một tên máy chủ mail khác (ví dụ: mail.example.com). Tên máy chủ mail này lại cần một bản ghi
A của riêng nó để phân giải ra địa chỉ IP. Nếu quản trị viên thay đổi địa chỉ IP của máy chủ web chính và chỉ cập nhật bản ghi **A** cho example.com, trang web có thể vẫn hoạt động bình thường, nhưng nếu họ quên cập nhật bản ghi **A** cho mail.example.com, dịch vụ email sẽ bị gián đoạn hoàn toàn. Điều này cho thấy việc quản lý DNS đòi hỏi sự hiểu biết toàn diện về các mối liên kết này để tránh những sự cố không đáng có.
Bảng sau đây cung cấp thông tin chi tiết về các loại bản ghi DNS phổ biến và quan trọng nhất:

Bảng 4.1: Bảng tra cứu các loại bản ghi DNS phổ biến

Loại Bản ghi	Tên đầy đủ	Chức năng	Cú pháp / Ví dụ
A	Address	Ánh xạ một tên miền (hostname) tới một địa chỉ IPv4 32-bit. Đây là bản ghi quan trọng nhất để một trang web có thể truy cập được.	example.com. IN A 93.184.216.34
AAAA	IPv6 Address	Tương tự bản ghi A,	example.com. IN AAAA

		nhưng ánh xạ tên miền tới một địa chỉ IPv6 128-bit.	2606:2800:220:1:248:1893:25c8:1946
CNAME	Canonical Name	Tạo một tên bí danh (alias) cho một tên miền khác (tên miền chính tắc). Mọi truy vấn đến tên bí danh sẽ được chuyển hướng đến tên miền chính. Hữu ích cho việc trỏ nhiều tên miền phụ vào cùng một máy chủ.	www.example.com. IN CNAME example.com.
MX	Mail Exchange	Chỉ định các máy chủ email chịu trách nhiệm nhận thư điện tử cho một tên miền. Có thể có nhiều bản ghi MX với các mức độ ưu tiên khác nhau (số nhỏ hơn có độ ưu tiên cao hơn).	example.com. IN MX 10 mail.example.com.
NS	Name Server	Ủy quyền một vùng DNS (hoặc một tên miền phụ) cho một tập hợp các máy chủ tên miền có thẩm quyền. Về cơ bản, nó cho biết "ai" chịu trách nhiệm về các bản ghi DNS cho tên miền này.	example.com. IN NS ns1.example.com.
SOA	Start of Authority	Chứa thông tin quản trị quan trọng về một vùng DNS, bao gồm máy chủ tên miền chính, email của quản trị viên, số serial của vùng, và các thông số thời gian (refresh, retry, expire, TTL). Mỗi vùng DNS phải có một bản ghi SOA.	example.com. IN SOA ns1.example.com. admin.example.com. (2023010101 7200 3600 1209600 3600)
TXT	Text	Cho phép quản trị viên lưu trữ các chuỗi văn bản tùy ý. Thường được sử dụng cho các mục đích xác thực như SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC để chống	example.com. IN TXT "v=spf1 include:_spf.google.com ~all"

		thư rác, hoặc để xác minh quyền sở hữu tên miền với các dịch vụ của bên thứ ba.	
PTR	Pointer	Thực hiện phân giải DNS ngược: ánh xạ một địa chỉ IP trở lại một tên miền. Chủ yếu được sử dụng trong các bản ghi của vùng in-addr.arpa (cho IPv4) và ip6.arpa (cho IPv6).	34.216.184.93.in-addr.arpa. IN PTR example.com.
SRV	Service	Chỉ định thông tin chi tiết (hostname, port, priority, weight) cho các dịch vụ cụ thể, ngoài các dịch vụ web và email tiêu chuẩn. Thường được sử dụng cho VoIP (Voice over IP), XMPP (chat), và các giao thức khác.	_sip._tcp.example.com. IN SRV 10 60 5060 bigbox.example.com.

Chương 5: Bảo mật DNS - Phòng thủ trước các Mối đe dọa Vô hình

Do vai trò trung tâm và thiết kế ban đầu vốn dựa trên sự tin cậy, DNS đã trở thành một mục tiêu hấp dẫn cho các tác nhân độc hại. Việc bảo vệ cơ sở hạ tầng DNS là cực kỳ quan trọng để đảm bảo an toàn và tin cậy cho toàn bộ Internet.

5.1. Các Lỗ hổng và Véc-tơ Tấn công Phổ biến

- **DNS Spoofing và Cache Poisoning (Giả mạo và Nhiễm độc bộ đệm DNS):** Đây là một trong những hình thức tấn công DNS nguy hiểm và phổ biến nhất. Kẻ tấn công sẽ lừa một DNS resolver chấp nhận và lưu trữ một bản ghi DNS giả mạo trong bộ nhớ đệm của nó. Khi một người dùng hợp pháp gửi truy vấn cho tên miền đã bị nhiễm độc, resolver sẽ trả về địa chỉ IP độc hại thay vì địa chỉ IP chính xác. Kết quả là người dùng bị chuyển hướng đến một trang web giả mạo (ví dụ: một trang đăng nhập ngân hàng giả) để đánh cắp thông tin nhạy cảm. Cuộc tấn công này khai thác một điểm yếu cơ bản trong thiết kế ban đầu của DNS, vốn không có cơ chế xác thực nguồn gốc của dữ liệu.
- **DNS Hijacking/Redirection (Chiếm quyền điều khiển/Chuyển hướng DNS):** Trong cuộc tấn công này, kẻ tấn công thay đổi cài đặt DNS trực tiếp trên máy tính của nạn nhân (thường thông qua phần mềm độc hại) để trỏ đến một máy chủ DNS do chúng kiểm soát. Một hình thức khác là chiếm quyền truy cập vào tài khoản quản lý tên miền và thay đổi các bản ghi NS có thẩm quyền, từ đó

chuyển hướng toàn bộ lưu lượng truy cập của tên miền đó.

- **DNS Tunneling (Tạo đường hầm qua DNS):** Kẻ tấn công lợi dụng giao thức DNS, vốn thường được các tường lửa cho phép đi qua, để tạo ra một kênh giao tiếp bí mật. Chúng mã hóa dữ liệu (chẳng hạn như lệnh điều khiển hoặc dữ liệu bị đánh cắp) vào trong các truy vấn và phản hồi DNS, qua mặt các biện pháp an ninh mạng truyền thống.
- **NXDOMAIN Attack (Tấn công Tên miền không tồn tại):** Đây là một dạng tấn công từ chối dịch vụ (Denial of Service - DoS). Kẻ tấn công tạo ra một lượng lớn các truy vấn DNS cho các tên miền phụ ngẫu nhiên và không tồn tại (ví dụ: asdfg.example.com, hjklp.example.com). Điều này buộc các DNS resolver phải làm việc cật lực để xác minh rằng các tên miền này không tồn tại, làm cạn kiệt tài nguyên của chúng và khiến chúng không thể phục vụ các truy vấn hợp pháp.

5.2. DNSSEC (DNS Security Extensions): Đảm bảo Tính toàn vẹn Dữ liệu

Để đối phó với các mối đe dọa giả mạo dữ liệu, một bộ mở rộng bảo mật gọi là DNSSEC đã được phát triển.

- **Nguyên tắc hoạt động:** DNSSEC không mã hóa các truy vấn DNS. Thay vào đó, nó sử dụng mật mã khóa công khai để tạo ra các *chữ ký số* cho các bản ghi DNS. Khi một DNS resolver nhận được một phản hồi, nó có thể sử dụng các chữ ký này để xác minh hai điều quan trọng: **tính xác thực** (dữ liệu thực sự đến từ máy chủ có thẩm quyền) và **tính toàn vẹn** (dữ liệu không bị thay đổi trên đường truyền).
- **Chuỗi Tin cậy (Chain of Trust):** DNSSEC hoạt động dựa trên một mô hình phân cấp gọi là "chuỗi tin cậy". Sự tin cậy bắt đầu từ vùng gốc (root zone), vốn được bảo mật thông qua các quy trình nghiêm ngặt. Vùng gốc sẽ ký và xác thực cho các vùng TLD (như .com). Các vùng TLD lại ký và xác thực cho các vùng tên miền cấp hai (như example.com). Chuỗi xác thực này tiếp tục đi xuống, tạo ra một đường dẫn tin cậy không thể phá vỡ từ gốc đến tên miền cuối cùng.
- **Các Bản ghi DNSSEC chính:** DNSSEC giới thiệu một số loại bản ghi mới để thực hiện việc ký và xác minh:
    - **DNSKEY:** Chứa khóa công khai (public key) của một vùng. Khóa này được sử dụng để xác minh các chữ ký. Có hai loại khóa chính là Zone Signing Key (ZSK) dùng để ký các bộ bản ghi (RRset) trong vùng, và Key Signing Key (KSK) dùng để ký chính bản ghi DNSKEY, tăng cường thêm một lớp bảo mật.
    - **RRSIG (Resource Record Signature):** Chứa chữ ký số được tạo ra cho một bộ bản ghi (RRset).
    - **DS (Delegation Signer):** Đây là bản ghi tạo ra liên kết trong chuỗi tin cậy. Nó chứa một bản băm (hash) của DNSKEY của vùng con và được đặt tại vùng cha. Khi một resolver được giới thiệu từ vùng cha đến vùng con, nó có thể so sánh bản hash trong bản ghi DS với DNSKEY của vùng con để xác thực.

5.3. Encrypted DNS: Đảm bảo Tính riêng tư Dữ liệu

Sự phát triển của các giao thức bảo mật DNS phản ánh một sự tiến hóa trong nhận thức về an ninh mạng. Ban đầu, mối đe dọa chính được xác định là việc dữ liệu có thể bị giả mạo, làm tổn hại đến *tính toàn vẹn*. DNSSEC ra đời để giải quyết vấn đề này, đảm bảo câu trả lời DNS là đúng và không bị thay đổi, nhưng bản thân truy vấn vẫn được gửi đi dưới dạng văn bản thuần túy. Khi nhận thức về giám sát hàng loạt và thu

thập dữ liệu tăng lên, việc các truy vấn DNS (tiết lộ mọi trang web người dùng truy cập) bị lộ ra đã trở thành một mối lo ngại lớn về *quyền riêng tư*. DoT và DoH được phát triển để giải quyết chính xác lỗ hổng này bằng cách mã hóa toàn bộ kênh giao tiếp, bảo vệ chống lại việc giám sát thụ động.

- **DNS-over-TLS (DoT):** Giao thức này mã hóa các truy vấn và phản hồi DNS bằng cách sử dụng Transport Layer Security (TLS), cùng một công nghệ bảo mật cho HTTPS. Lưu lượng DoT được gửi qua một cổng mạng chuyên dụng là cổng 853. Điều này giúp ngăn chặn hiệu quả việc nghe lén và tấn công xen giữa (man-in-the-middle) trên đường truyền.
- **DNS-over-HTTPS (DoH):** Giao thức này cũng mã hóa lưu lượng DNS, nhưng thay vì sử dụng một cổng riêng, nó gói các truy vấn DNS bên trong các yêu cầu HTTPS thông thường và gửi chúng qua cổng 443. Lợi thế của phương pháp này là lưu lượng DNS được "ngụy trang" và hòa lẫn vào hàng tỷ yêu cầu HTTPS khác, khiến việc phát hiện, phân tích và chặn nó trở nên khó khăn hơn nhiều so với DoT.

Cuộc tranh luận giữa DoT và DoH cũng cho thấy một sự giằng co về quyền kiểm soát: ai sẽ có khả năng giám sát lưu lượng DNS? Với DoT, quản trị viên mạng doanh nghiệp có thể dễ dàng xác định và quản lý lưu lượng DNS được mã hóa. Với DoH, quyền kiểm soát đó có xu hướng chuyển sang các ứng dụng (như trình duyệt) và người dùng cuối, gây khó khăn cho việc thực thi các chính sách bảo mật của doanh nghiệp.

Bảng 5.1: So sánh DNS-over-TLS (DoT) và DNS-over-HTTPS (DoH)

Tiêu chí	DNS-over-TLS (DoT)	DNS-over-HTTPS (DoH)
Giao thức nền	Gói DNS trực tiếp trong TLS	Gói DNS trong HTTP, sau đó gói trong TLS
Cổng mặc định	853	443 (cùng cổng với HTTPS)
Mức độ hiển thị trên mạng	Dễ nhận biết vì sử dụng cổng riêng. Quản trị viên mạng có thể thấy lưu lượng DoT đang diễn ra (nhưng không đọc được nội dung).	Khó nhận biết, hòa lẫn với lưu lượng web HTTPS thông thường.
Khả năng bị chặn	Dễ bị chặn hơn ở cấp độ mạng bằng cách chặn cổng 853.	Rất khó chặn mà không ảnh hưởng đến toàn bộ lưu lượng web HTTPS.
Trường hợp sử dụng chính	Môi trường doanh nghiệp, mạng được quản lý, nơi cần sự cân bằng giữa mã hóa và khả năng giám sát.	Người dùng cá nhân ưu tiên quyền riêng tư tối đa, các ứng dụng (trình duyệt), và để vượt qua các rào cản kiểm duyệt DNS.
Ưu điểm	Hiệu suất cao hơn một chút (ít lớp giao thức hơn), dễ quản lý và giám sát hơn cho quản trị viên mạng.	Quyền riêng tư cao hơn (ngụy trang tốt hơn), khó bị chặn hơn.
Nhược điểm	Dễ bị chặn hơn, ít "ẩn mình" hơn.	Có thể bị lạm dụng bởi phần mềm độc hại để ẩn giao tiếp, gây khó khăn cho việc thực thi chính sách bảo mật của doanh nghiệp, hiệu suất thấp hơn một chút do có thêm lớp HTTP.

Chương 6: Quản lý và Gỡ lỗi DNS trong Thực tế

Việc hiểu lý thuyết về DNS là quan trọng, nhưng khả năng áp dụng kiến thức đó để cấu hình, quản lý và khắc phục sự cố trong các tình huống thực tế là kỹ năng không thể thiếu đối với bất kỳ quản trị viên hệ thống hay người dùng nâng cao nào.

6.1. Lựa chọn và Cấu hình DNS Server

Người dùng có quyền lựa chọn máy chủ DNS mà họ muốn sử dụng. Việc này có thể cải thiện tốc độ, tăng cường bảo mật hoặc cho phép truy cập vào các tính năng lọc nội dung.

- **Các nhà cung cấp Public DNS phổ biến:**
  - **Quốc tế:**
    - **Google Public DNS:** 8.8.8.8 và 8.8.4.4
    - **Cloudflare DNS:** 1.1.1.1 và 1.0.0.1
    - **OpenDNS:** 208.67.222.222 và 208.67.220.220
    - **Quad9:** 9.9.9.9 và 149.112.112.112
  - **Việt Nam:**
    - **VNPT:** 203.162.4.191 và 203.162.4.190
    - **Viettel:** 203.113.131.1 và 203.113.131.2
    - **FPT:** 210.245.24.20 và 210.245.24.22
- Hướng dẫn thay đổi DNS Server:
  Quá trình thay đổi DNS Server thường được thực hiện trong cài đặt mạng của hệ điều hành hoặc router. Các bước cơ bản như sau 6:
  1. Mở Control Panel (trên Windows) hoặc System Preferences (trên macOS).
  2. Điều hướng đến phần cài đặt mạng (Network and Sharing Center hoặc Network).
  3. Chọn kết nối mạng đang hoạt động (Wi-Fi hoặc Ethernet) và mở phần thuộc tính (Properties).
  4. Tìm đến mục Internet Protocol Version 4 (TCP/IPv4) và/hoặc Version 6 (TCP/IPv6).
  5. Chọn tùy chọn "Use the following DNS server addresses" và nhập địa chỉ IP của máy chủ DNS chính (Preferred) và phụ (Alternate) mà bạn muốn sử dụng.
  6. Lưu lại các thay đổi.

6.2. Công cụ Gỡ lỗi Dòng lệnh: dig và nslookup

Khi gặp sự cố liên quan đến DNS, các công cụ dòng lệnh là phương pháp hiệu quả nhất để chẩn đoán vấn đề.

- **dig (Domain Information Groper):**
  - **Giới thiệu:** dig là công cụ mạnh mẽ, linh hoạt và được các chuyên gia mạng ưa chuộng. Nó có sẵn trên hầu hết các hệ điều hành Linux và macOS và có thể được cài đặt trên Windows. dig cung cấp đầu ra chi tiết, có cấu trúc, rất phù hợp cho việc phân tích sâu và viết kịch bản tự động hóa.
  - **Cài đặt:**
    - Trên Debian/Ubuntu: sudo apt install dnsutils.
    - Trên CentOS/RHEL: sudo yum install bind-utils.

        - Trên Windows: Tải về bộ công cụ BIND từ trang web của ISC và chọn cài đặt "Tools Only".
    - **Ví dụ Thực hành:**
        - **Truy vấn cơ bản (A record):** dig example.com.
        - **Truy vấn các loại bản ghi cụ thể:** dig example.com MX để tra cứu bản ghi MX, hoặc NS, TXT, SOA.
        - **Truy vấn một DNS server cụ thể:** dig @8.8.8.8 example.com.
        - **Tra cứu ngược (Reverse lookup):** dig -x 8.8.8.8.
        - **Theo dõi đường đi của truy vấn:** dig example.com +trace sẽ hiển thị từng bước của quá trình phân giải, từ máy chủ gốc đến máy chủ có thẩm quyền.
        - **Rút gọn đầu ra:** dig example.com +short chỉ hiển thị giá trị của bản ghi (ví dụ: địa chỉ IP).
        - **Truy vấn hàng loạt từ file:** dig -f domains.txt, trong đó domains.txt là một tệp chứa danh sách các tên miền cần truy vấn, mỗi tên miền trên một dòng.
- **nslookup (Name Server Lookup):**
    - **Giới thiệu:** nslookup là một công cụ cũ hơn nhưng vẫn rất hữu ích, đặc biệt là vì nó được cài đặt sẵn trên hệ điều hành Windows. Nó có hai chế độ hoạt động: không tương tác (để tra cứu nhanh) và tương tác (để thực hiện nhiều truy vấn liên tiếp).
    - **Ví dụ Thực hành:**
        - **Chế độ không tương tác:** nslookup example.com.
        - **Chế độ tương tác:** Gõ nslookup và nhấn Enter. Tại dấu nhắc >, bạn có thể nhập các lệnh như set type=mx rồi sau đó nhập google.com để tra cứu bản ghi MX.
        - **Truy vấn các loại bản ghi:** nslookup -type=soa example.com.
        - **Sử dụng một DNS server khác:** nslookup example.com 8.8.8.8.
        - **Tra cứu ngược:** nslookup 8.8.8.8.

6.3. So sánh các Công cụ: dig vs. nslookup vs. host

Việc lựa chọn công cụ gỡ lỗi DNS không chỉ là vấn đề sở thích mà còn phản ánh sự khác biệt cơ bản về cách chúng hoạt động. nslookup được biết là sử dụng thư viện resolver của riêng nó, tách biệt với hệ điều hành, trong khi dig và host thường sử dụng các thư viện resolver tiêu chuẩn của hệ thống. Điều này có một hàm ý quan trọng:
nslookup có thể trả về một kết quả thành công trong khi các ứng dụng khác trên cùng hệ thống (như trình duyệt) lại gặp lỗi phân giải, và ngược lại. Bởi vì nslookup không đi theo cùng một "đường dẫn mã" (code path) như các ứng dụng hệ thống, kết quả của nó có thể không phản ánh chính xác 100% những gì đang thực sự xảy ra. Do đó, khi gỡ lỗi, dig được coi là một công cụ chẩn đoán đáng tin cậy hơn vì nó mô phỏng gần hơn cách hệ thống thực sự phân giải tên miền.

- **nslookup:** Từng bị coi là lỗi thời nhưng đã được "hồi sinh". Điểm mạnh lớn nhất của nó là tính sẵn có mặc định trên Windows, rất tiện lợi cho việc kiểm tra nhanh. Tuy nhiên, kết quả của nó có thể gây hiểu lầm trong một số trường hợp phức tạp do cơ chế resolver nội bộ.
- **dig:** Là "tiêu chuẩn vàng" cho các chuyên gia mạng. Nó cung cấp đầu ra cực kỳ chi tiết, có cấu trúc rõ ràng, dễ phân tích và lý tưởng cho việc gỡ lỗi sâu cũng như tự động hóa các tác vụ kiểm tra DNS.
- **host:** Là công cụ đơn giản nhất, cung cấp đầu ra ngắn gọn và dễ đọc. Nó rất phù hợp cho các kiểm tra nhanh chóng (ví dụ: "tên miền này có phân giải ra IP không?") hoặc để sử dụng trong các kịch

bản (script) đơn giản.

Kết luận

Hệ thống Phân giải Tên miền (DNS) là một kỳ công kỹ thuật thầm lặng, một trụ cột thiết yếu đã cho phép Internet phát triển từ một mạng lưới nghiên cứu nhỏ thành một nền tảng toàn cầu. Thông qua kiến trúc cây phân cấp và cơ chế ủy quyền thông minh, DNS đã giải quyết thành công bài toán về quy mô và quản lý phân tán, tạo ra một hệ thống vừa linh hoạt, vừa có khả năng phục hồi cao. Nó không chỉ đơn thuần là một "danh bạ" mà còn là một lớp trừu tượng chiến lược, tách biệt danh tính và vị trí, cho phép các công nghệ web hiện đại như CDN và cân bằng tải hoạt động một cách liền mạch.

Hành trình của một truy vấn DNS, từ máy khách đến máy chủ gốc, TLD, và cuối cùng là máy chủ có thẩm quyền, cho thấy một vũ điệu phức tạp của các tương tác đệ quy và lặp, được tối ưu hóa bằng cơ chế bộ nhớ đệm. Trái tim của hệ thống này là các bản ghi DNS—ngôn ngữ chung cho phép định cấu hình và quản lý mọi khía cạnh của một tên miền, từ trang web, email cho đến các dịch vụ chuyên biệt.

Tuy nhiên, sự tin cậy vốn có trong thiết kế ban đầu cũng khiến DNS trở thành một mục tiêu tấn công. Sự phát triển từ DNSSEC, tập trung vào tính toàn vẹn của dữ liệu, đến các giao thức mã hóa như DoT và DoH, tập trung vào quyền riêng tư của truy vấn, đã cho thấy một sự tiến hóa tất yếu trong nhận thức về an ninh mạng. Cuộc tranh luận giữa DoT và DoH cũng nêu bật sự cân bằng tinh tế giữa khả năng kiểm soát của quản trị viên mạng và quyền riêng tư của người dùng cuối—một chủ đề sẽ tiếp tục định hình tương lai của Internet.

Cuối cùng, việc nắm vững các công cụ thực hành như dig và nslookup là kỹ năng không thể thiếu, cho phép chúng ta không chỉ hiểu lý thuyết mà còn có thể chẩn đoán và giải quyết các vấn đề trong thế giới thực. Từ những khái niệm cơ bản đến các giao thức bảo mật tiên tiến, việc hiểu rõ DNS chính là hiểu rõ một phần linh hồn của mạng Internet.