BỘ KHOA HỌC VÀ CÔNG NGHỆ
**TRUNG TÂM INTERNET VIỆT NAM**

# DNS WORKSHOP (VIC 2025)

**Hà Nội, 07/2025**

# NỘI DUNG

- Tổng quan và hiện trạng
- Lý thuyết cơ bản; Nguyên lý hoạt động
- Hướng dẫn cài đặt, thiết lập, quản trị, vận hành
- Mô hình tiêu chuẩn
- Hướng dẫn tối ưu hóa, bảo mật
- DNS IPv6
- DNSSEC

# I. TỔNG QUAN VÀ HIỆN TRẠNG

# Nội dung

- Tổng quan về hệ thống DNS và ứng dụng
- Xu hướng phát triển của DNS
- Tổng quan tình hình triển khai DNS của CQNN

# Tổng quan về hệ thống DNS và ứng dụng

- **Sự phổ biến và ứng dụng rộng rãi:**
  - DNS đóng vai trò thiết yếu trong hoạt động của Internet, được ứng dụng rộng rãi trên toàn cầu.
  - Hầu hết mọi hoạt động trực tuyến đều dựa trên việc sử dụng DNS để phân giải tên miền thành địa chỉ IP.
- **Tăng trưởng của tên miền:**
  - Số lượng tên miền đăng ký liên tục tăng lên.
  - Điều này dẫn đến áp lực lớn lên hệ thống DNS toàn cầu
- **Các thách thức:**
  - Đảm bảo tính ổn định, khả sẵn sàng và khả năng mở rộng của hệ thống DNS.
  - Ngăn chặn các cuộc tấn công vào hệ thống DNS như DDoS, DNS spoofing.
  - Quản lý và điều phối hệ thống DNS toàn cầu một cách hiệu quả.

# Xu hướng phát triển của DNS (1/2)

- Số lượng kết nối thông qua DNS sẽ tăng lên rất nhiều lần, yêu cầu về chất lượng cần phải đảm bảo như tốc độ kết nối nhanh và trong suốt với người dùng

- Tính riêng tư và an toàn của người dùng khi sử dụng DNS sẽ được quan tâm nhiều hơn và việc đảm bảo sự tin cậy trong các kết nối, độ tin cậy cho dịch vụ của người dùng thông qua sử dụng phân giải tên miền vẫn là những yếu tố quan trọng cốt lõi.

# Xu hướng phát triển của DNS (2/2)

- DNS đóng vai trò quan trọng trong hoạt động của Internet và đang không ngừng phát triển để đáp ứng nhu cầu ngày càng tăng của người dùng và các ứng dụng dịch vụ chuyển đổi số quốc gia. Xu hướng phát triển của DNS trong tương lai sẽ được định hình theo các yếu tố sau:
  - **Tăng trưởng về cơ sở dữ liệu tên miền:** Với sự phát triển nhanh chóng của Internet kéo theo sự tăng trưởng mạnh về số lượng dịch vụ trực tuyến, kéo theo số lượng tên miền gia tăng, đặt ra nhu cầu phát triển hạ tầng DNS để đáp ứng.
  - **Độ trễ thấp:** Các hệ thống DNS liên tục cải thiện hiệu suất và độ tin cậy của hệ thống, bằng cách nâng cấp hạ tầng, tối ưu hóa lưu lượng và áp dụng các kỹ thuật mới như DNS over HTTPS (DoH).
  - **Bảo mật và quyền riêng tư:** Bảo mật và quyền riêng tư của người dùng ngày càng được chú trọng, thúc đẩy việc áp dụng các giải pháp mã hóa và bảo mật mạnh mẽ hơn trong DNS.
  - **Nâng cao khả năng đáp ứng và mở rộng:** DNS đang được mở rộng để ứng dụng đáp ứng, tương thích với các vấn đề như an ninh mạng, lưu trữ phân tán, IoT và nhiều ứng dụng khác.

# Tổng quan tình hình triển khai DNS của CQNN

- Có hệ thống máy chủ DNS riêng, hoặc thuê Hosting tại doanh nghiệp hoặc dịch vụ Hosting tại nước ngoài.
- Chưa chú trọng đến thiết kế mô hình chuẩn, đảm bảo an toàn, dự phòng.
- Chưa triển khai các giải pháp công nghệ nhằm tăng cường đảm bảo an toàn như ký DNSSEC, IPv6, cân bằng tải, …
- Có nhiều điểm yếu về an toàn trong quản lý, cấu hình kỹ thuật cho máy chủ (chưa cấu hình ẩn phiên bản phần mềm DNS, cho phép đồng bộ dữ liệu ra bên ngoài, ….)
- Sử dụng DNS Cache miền phí của nước ngoài như Google, Cloudflare, …
- Không có hệ thống DNS Cache dự phòng hoặc sử dụng chung với hệ thống DNS Authoritative.

# II. LÝ THUYẾT CƠ BẢN

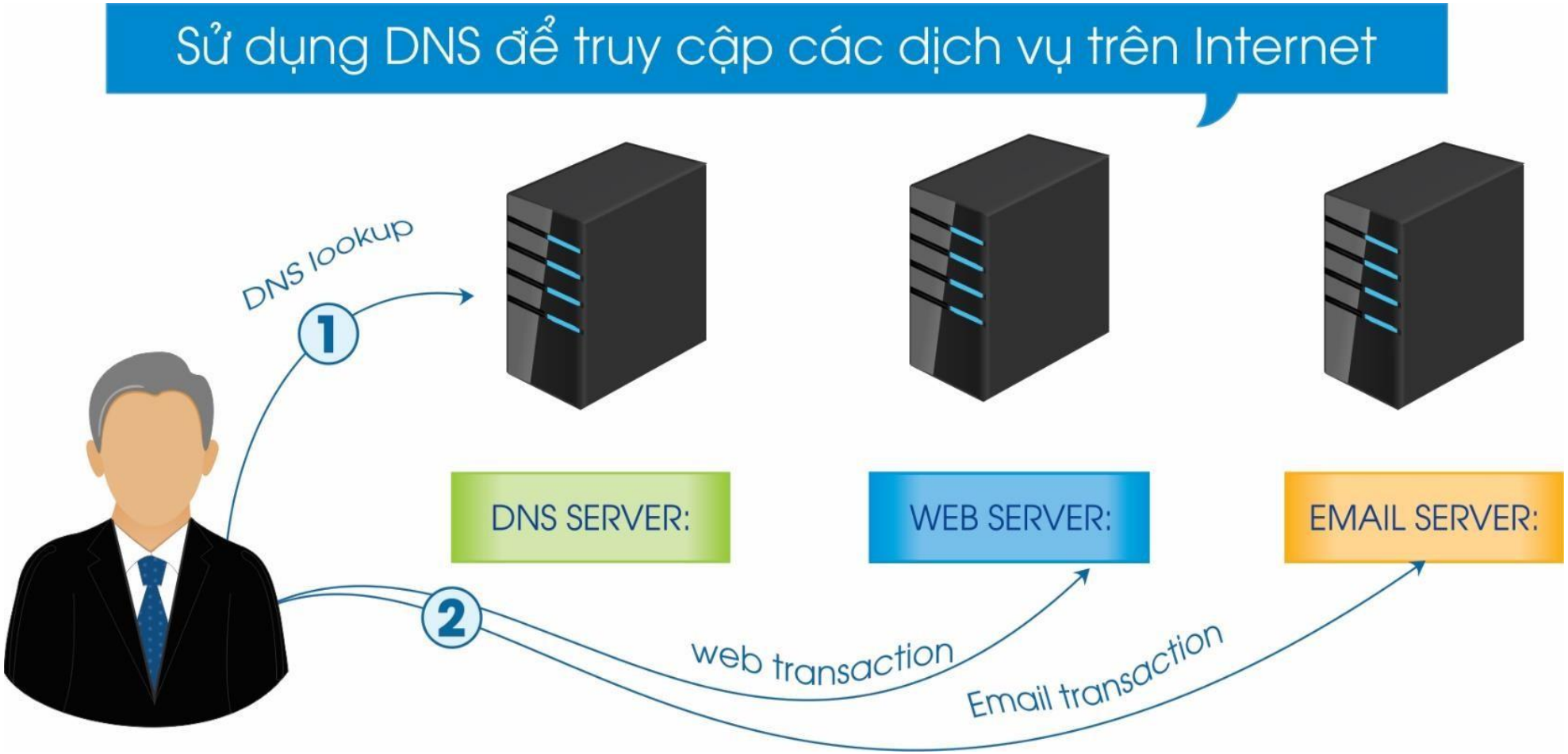
# Nội dung

- Vai trò, chức năng của DNS
- Đặc điểm của DNS
- Thành phần cơ bản của DNS
  - Không gian tên miền
  - Máy chủ tên miền
  - Resolver
  - File dữ liệu và các bản ghi tài nguyên
  - Các file dữ liệu đặc biệt
- Bản ghi tài nguyên
  - A, AAA, NS, MX, PTR
- Phân loại máy chủ
  - Máy chủ tên miền
  - DNS Cache
  - DNS Stealth, DNS Forwarder, DNS Hybrid
- Hoạt động của DNS
  - Chuyển giao
  - Đồng bộ dữ liệu
  - Ánh xạ tên miền
  - Truy vấn tên miền
  - Phân giải tên miền

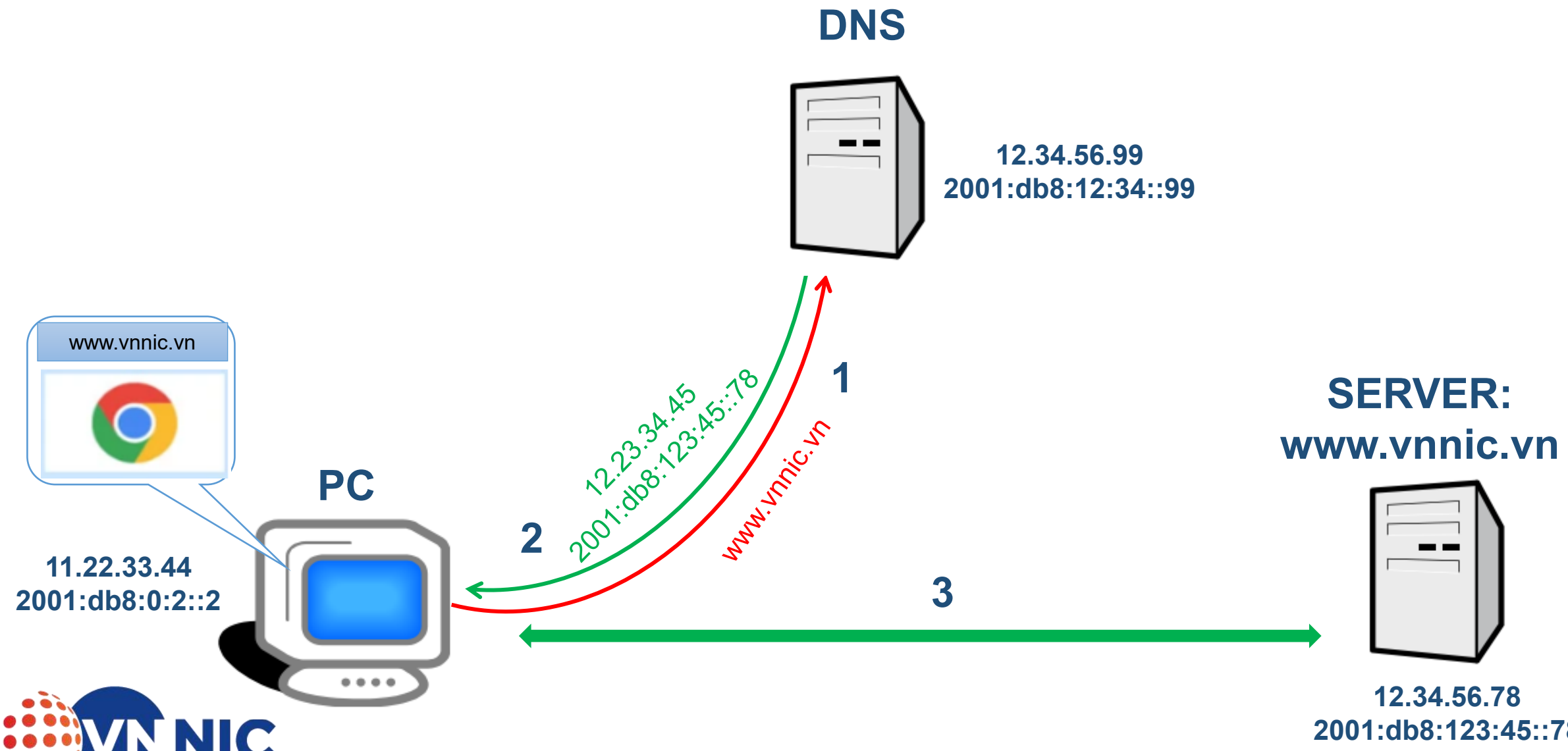
# Chức năng của DNS

- DNS (**D**omain **N**ame **S**ystem): Hệ thống tên miền, thực hiện chức năng:
  - Ánh xạ tên miền sang địa chỉ IP, cho phép người dùng truy cập vào các trang web bằng cách nhập tên miền thay vì nhớ địa chỉ IP dài và khó nhớ.
  - Ánh xạ ngược từ IP sang tên miền, xác định tên miền của một địa chỉ IP cụ thể, sử dụng cho một số yêu cầu xác thực (ví dụ hệ thống Email, thiết bị mạng, …)
  - Cung cấp thông tin bổ sung phục vụ cho các hoạt động của hệ thống, ví dụ thông tin máy chủ Email, máy chủ quản lý tên miền, lưu trữ thông tin văn bản, …

# Vai trò của DNS



# Truy cập dịch vụ Website



# Đặc điểm của DNS (1/2)

- Hệ thống tên miền là một cơ sở dữ liệu phân bố toàn cầu.
- Cơ sở dữ liệu này cho phép quản lý một cách cục bộ các phần khác nhau trong toàn bộ hệ thống tên miền.
- Dữ liệu trong mỗi phần này có thể được truy cập trên toàn mạng thông qua cơ chế client-server.

# Đặc điểm của DNS (2/2)

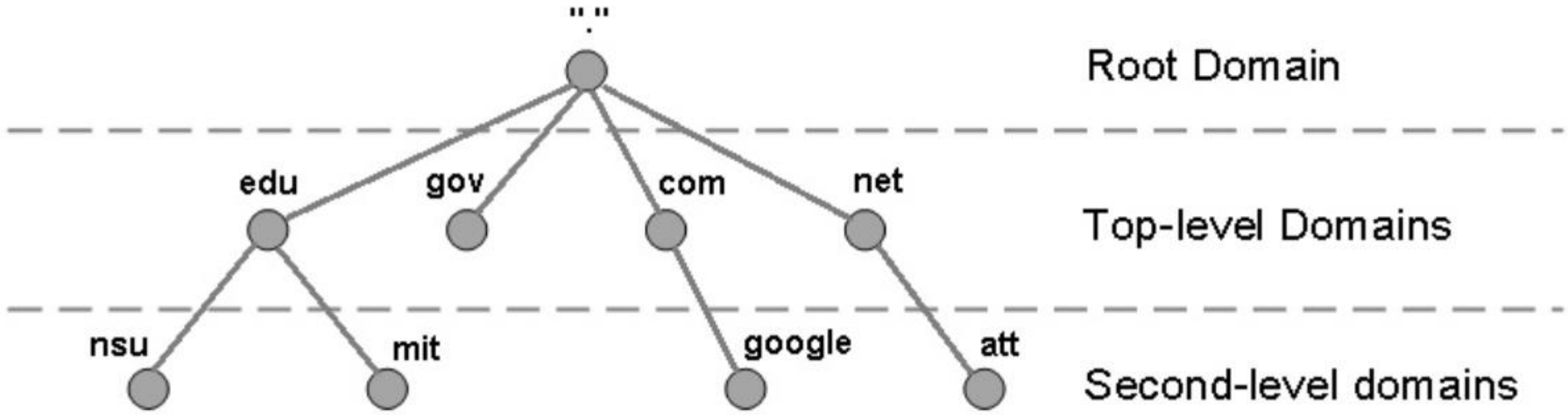
- **Tổ chức phân cấp hình cây**
  - Mỗi máy chủ quản lý một số tên miền nhất định.
  - Có khả năng truy vấn từ bất kỳ đâu mà không cần kết nối trực tiếp.
  - Dữ liệu tên miền có thể được lưu tạm trong bộ nhớ “cache” để tăng khả năng hoạt động của hệ thống
- **Liên kết chặt chẽ, độ tin cậy cao**
  - Một tên miền có thể được quản lý bởi nhiều máy chủ khác nhau
  - Có cơ chế đồng bộ đảm bảo dữ liệu thống nhất.
  - Dữ liệu có thể cập nhật tự động, tức thời.
  - Chỉ cần cập nhật vào máy chủ chính, máy chủ phụ sẽ tự động đồng bộ
- **Quản lý dữ liệu:**
  - Có khả năng quản lý số lượng lớn tên miền.
  - Dữ liệu có thể lưu vào file hoặc cơ sở dữ liệu.

# Thành phần cơ bản của DNS

- Không gian tên miền
- Máy chủ tên miền
- Resolver
- File dữ liệu và các bản ghi tài nguyên

# Không gian tên miền

- Không gian tên miền (Domain Name Space) là toàn bộ cơ sở dữ liệu tên miền.



# Tên miền (Domain Name)

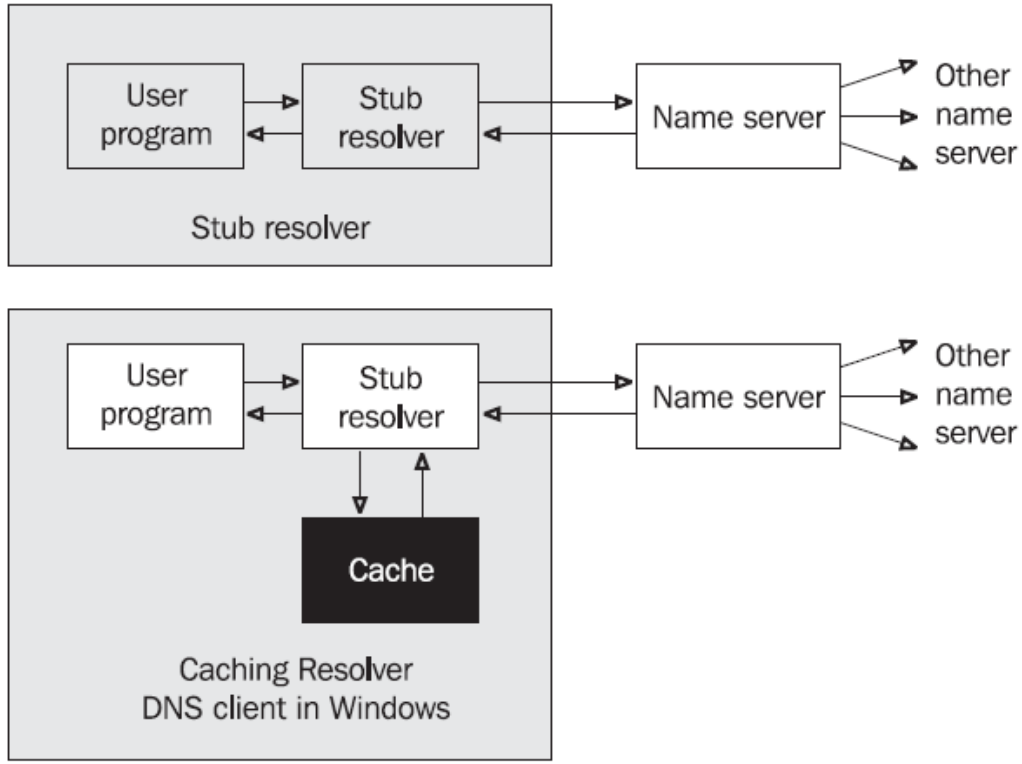
- Tên miền đầy đủ của 1 node trên cây tên miền (FQDN: Fully Qualified Domain Name):
  - Thể hiện vị trí của node trong không gian tên miền.
  - Là một chuỗi các nhãn trên đường đi từ node đến gốc Root của cây tên miền, được phân cách nhau bằng dấu chấm “.” và kết thúc bằng dấu chấm “.”. Các tên miền không được kết thúc bằng dấu chấm ở cuối tên miền được xem như tạo từ một node khác không phải là root.
- Cách đọc tên miền là đọc theo chiều từ trái qua phải của tên miền (đọc các nhãn từ node đến Root).
- Ví dụ tên miền đầy đủ: www.example.vn., www.vnnic.vn., mic.gov.vn.

# Máy chủ tên miền

- Máy chủ tên miền (Name Server):
  - Là máy chủ triển khai chương trình lưu trữ thông tin về các không gian tên miền.
  - Có đầy đủ thông tin về một hoặc số phần của không gian tên miền (zone).
  - Máy chủ tên miền có toàn quyền đối với phần không gian tên miền (zone) mà máy chủ quản lý.

# Resolver

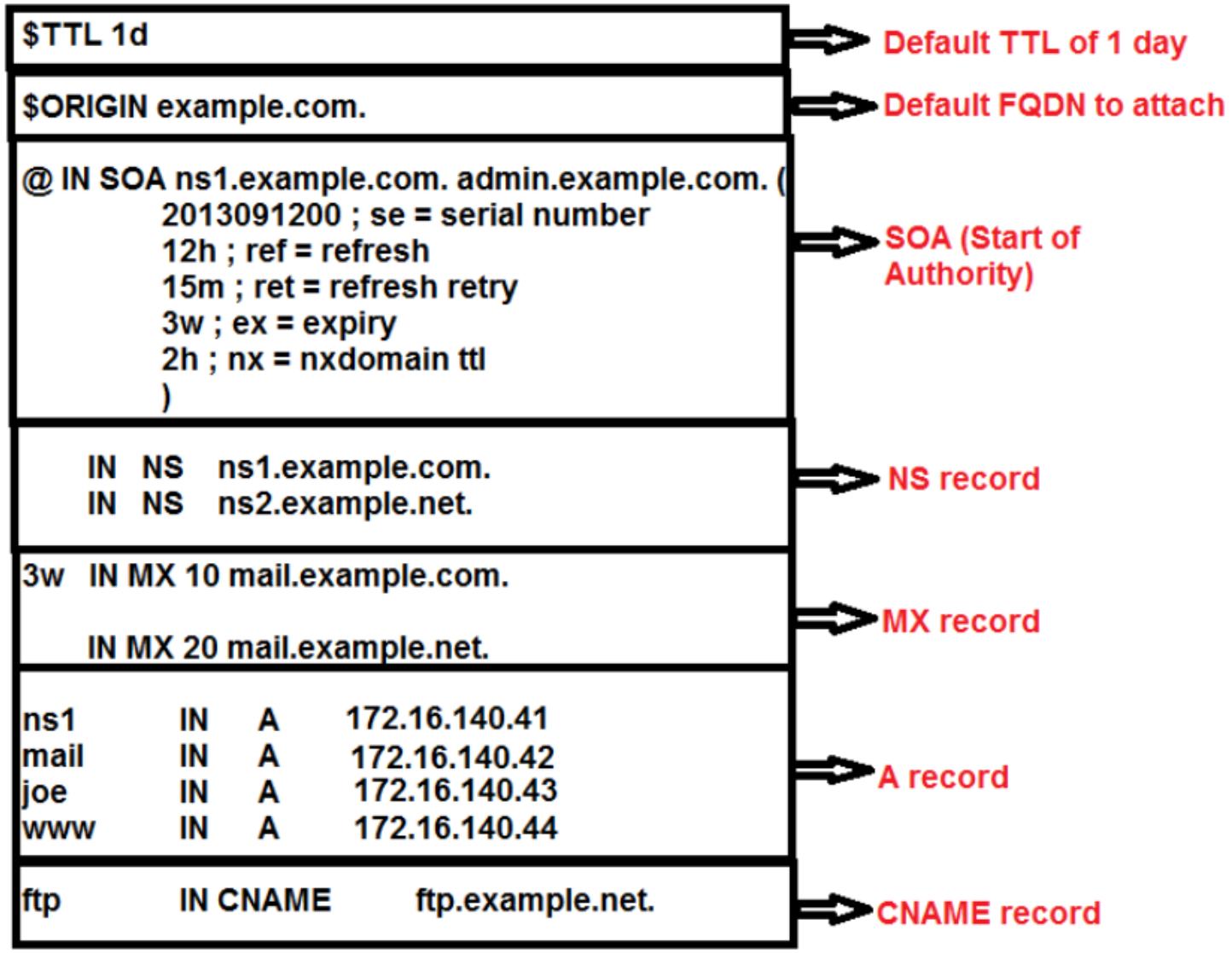
- Resolver là chương trình được thiết lập trên máy chủ phía Client.
- Resolver thực hiện chức năng tương tác với chương trình ứng dụng và các máy chủ tên miền, tạo ra các yêu cầu phân giải tên miền đến các máy chủ tên miền.
- Chương trình Resolver có thể hỗ trợ thêm tính năng lưu cache, được gọi là DNS Client, tính năng này được hiểu rằng các thông tin về câu trả lời nhận được từ các máy chủ tên miền sẽ được lưu lại trong một khoảng thời gian, giúp cho hoạt động truy vấn tên miền nhanh chóng, giảm tải cho các máy chủ.



# File dữ liệu và các bản ghi tài nguyên (1/2)

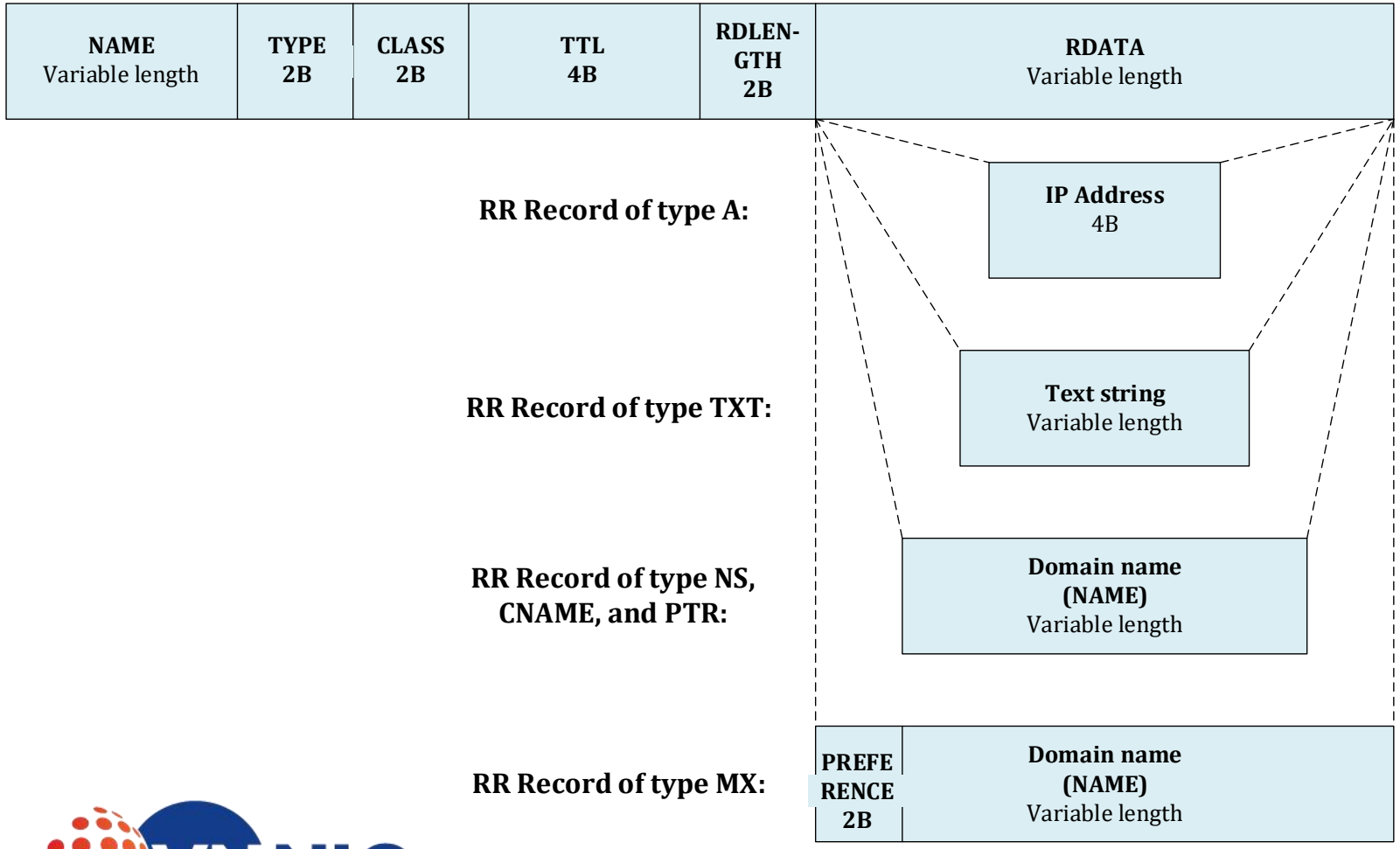
- File dữ liệu là file lưu trữ các thông tin về các dữ liệu tên miền.
- Thông tin về dữ liệu tên miền được đưa vào định dạng gọi là bản ghi tài nguyên (**R**esource **R**ecord: RR), trong bản ghi này khai báo các bản ghi ánh xạ tên miền hoặc IP sang các dạng thông tin tương ứng tùy thuộc vào mục đích sử dụng.
- Các bản ghi này được phân chia theo từng lớp (Class).
  - Mỗi lớp liên quan đến một hệ thống nhất định
  - Có các loại lớp như: IN (Internet); CH (Chaos); HS (Hesiod)
  - Lớp IN (Internet ) là thông dụng hơn cả.
- Trong lớp Internet (IN) có 1 số loại bản ghi tên miền quan trọng và phổ biến như sau: SOA, NS, A, AAAA, MX, TXT, PTR, ngoài ra còn có rất nhiều bản ghi tên miền khác như CNAME, WKS, HIFO, …
- 1 số khai báo chỉ thị trong file dữ liệu: $TTL, $INCLUDE, $GENERATE, $ORIGIN

# File dữ liệu và các bản ghi tài nguyên (2/2)



# Cấu trúc bản ghi tài nguyên

- Cấu trúc của bản ghi tài nguyên như sau:




- TTL: Thông tin lưu trữ bản ghi trên các máy chủ truy vấn tên miền.
- Class: Không gian sử dụng tên miền, thông thường sử dụng trong trường Internet với Class là IN.
- Type: Loại bản ghi tài nguyên
- Rdata: Dữ liệu ánh xạ với tên miền

# Bản ghi SOA

- SOA (**S**tart **o**f **A**uthority) là bản ghi chỉ định thông tin có thẩm quyền về zone tên miền, 01 zone tên miền chỉ có duy nhất 01 bản ghi SOA.
- Rdata của bản ghi SOA gồm thông tin
  - Máy chủ tên miền
  - Mail quản trị zone tên miền
  - Serial tên miền phục vụ đồng bộ dữ liệu giữa Master và Slave
  - Một số bộ định thời liên quan đến cập nhật zone tên miền

# Bản ghi NS

- NS (**N**ame **S**erver): Bản ghi lưu trữ thông tin chuyển giao, Rdata là thông tin máy chủ tên miền được chuyển giao quản lý zone tên miền, là các máy chủ quản lý các bản ghi tài nguyên của tên miền.

- Bản ghi NS được khai báo trên máy chủ tên miền quản lý zone tên miền (zone con) và máy chủ thực hiện chuyển giao (zone cha)

- Cấu trúc bản ghi NS:

| domain | TTL | Class | NS | name.server |
|---|---|---|---|---|

- Ví dụ bản ghi NS của tên miền example.vn.

| | | | | |
|---|---|---|---|---|
| example.vn. | 3600 | IN | NS | ns1.example.vn. |
| example.vn. | 3600 | IN | NS | ns2.example.vn. |

  - Trong ví dụ, tên miền example.vn. được chuyển giao cho 02 máy chủ ns1.example.vn và ns2.example.vn quản lý.

  - 02 bản ghi NS này được khai báo trên máy chủ quản lý zone tên miền .vn (zone cha của zone example.vn) và trên máy chủ quản lý zone tên miền example.vn (zone con)

# Bản ghi A

- Bản ghi A là bản ghi khai báo thông tin địa chỉ IPv4 của tên miền, Rdata là địa chỉ IPv4.
- Cấu trúc bản ghi A:

| domain | TTL | Class | A | IPv4 |
|---|---|---|---|---|

- Ví dụ bản ghi A của tên miền example.vn:

| example.vn. | 3600 | IN | A | 192.168.10.25 |
|---|---|---|---|---|

  - Thông tin khai báo được hiểu rằng tên miền example.vn được ánh xạ đến địa chỉ IPv4 192.168.10.25

# Bản ghi AAAA

- Bản ghi AAAA là bản ghi khai báo thông tin địa chỉ IPv6 của tên miền, Rdata là địa chỉ IPv6.
- Cấu trúc bản ghi AAAA:

| domain | TTL | Class | AAAA | IPv6 |
|---|---|---|---|---|

- Ví dụ bản ghi AAAA của tên miền example.vn:

| example.vn. | 3600 | IN | AAAA | 2001:dc8:0:1::100 |
|---|---|---|---|---|

  - Thông tin khai báo được hiểu rằng tên miền example.vn được ánh xạ đến địa chỉ IPv4 2001:dc8:0:1::100

# Bản ghi MX

- Bản ghi MX khai báo trạm chuyển tiếp thư điện tử, lưu trữ thông tin máy chủ Mail của tên miền, Rdata lưu trữ tên máy chủ Mail và thông tin về sự ưu tiên của máy chủ Mail.
- Cấu trúc:

| Domain | TTL | Class | MX | prefer | mail.server |
|---|---|---|---|---|---|

- Ví dụ về bản ghi MX của tên miền example.vn.

| | | | | | |
|---|---|---|---|---|---|
| example.vn. | 3600 | IN | MX | 10 | mail01.example.vn. |
| example.vn. | 3600 | IN | MX | 20 | mail02.example.vn. |

  - Thông tin khai báo bản ghi MX như trên được hiểu rằng khi gửi email đến địa chỉ user@exampe.vn thì thư điên tử được gửi đến 02 máy chủ Mail mail01.example.vn và mail02.example.vn
  - Trong đó mail01.example.vn có giá trị ưu tiên là 10, mail02.example.vn có giá trị ưu tiên là 20, máy chủ mail có giá trị ưu tiên thấp hơn thì được ưu tiên hơn (giá trị ưu tiên có thể sử dụng 1-255)

# Bản ghi PTR

- Bản ghi PTR cho phép khai báo thông tin ánh xạ từ địa chỉ IP sang địa chỉ tên miền, IPV4/IPv6 được đưa vào dưới định dạng tên miền, Rdata là bản ghi tên miền. Nhiều hệ thống (đặc biệt là Mail Server) sử dụng ánh xạ ngược để thực hiện kiểm tra xác thực và an toàn.
- Cấu trúc bản ghi tên miền ngược IPv4:

| a.b.c.d.in-addr.arpa. | TTL | IN | PTR | domain |
|---|---|---|---|---|

- Cấu trúc bản ghi tên miền ngược IPv6:

| ……..ipv6.arpa. | TTL | IN | PTR | domain |
|---|---|---|---|---|

- Ví dụ bản ghi PTR:

| 25.10.168.192.in-addr.arpa. | 3600 | IN | PTR | example.vn. |
|---|---|---|---|---|
| 0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.8.c.d.0.1.0.0.2.ipv6.arpa. | 3600 | IN | PTR | example.vn. |

  - Thông tin bản ghi PTR được hiểu IPv4 192.168.10.25 và IPv6 2001:dc8:0:1::100 được ánh xạ đến tên miền example.vn.

# Phân loại máy chủ

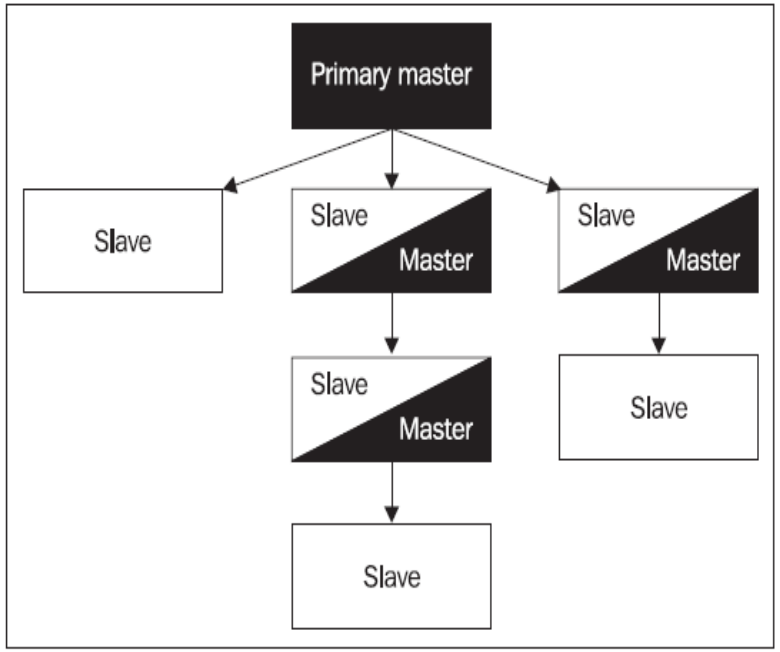
- Name Server (máy chủ tên miền)
- DNS Cache
- DNS Stealth
- DNS Forwarder
- DNS Hybrid

# Máy chủ tên miền

- Máy chủ tên miền (Name Server) có chương trình quản lý, lưu trữ các thông tin về không gian tên miền, zone tên miền được chuyển giao, cụ thể là các bản ghi tên miền của zone quản lý, được gọi là máy chủ Authoritatve (máy chủ thẩm quyền) với zone tên miền quản lý.
- Máy chủ tên miền thực hiện chức năng tiếp nhận yêu cầu cung cấp thông tin về tên miền và trả lời thông tin về tên miền theo yêu cầu (sau đây được gọi là phân giải tên miền bao gồm: truy vấn tên miền và phản hồi truy vấn tên miền).
- Một máy chủ tên miền có thể có quyền trên nhiều Zone.
- Đối với 1 zone tên miền có 02 loại máy chủ tên miền: máy chủ tên miền Master và máy chủ tên miền Slave.

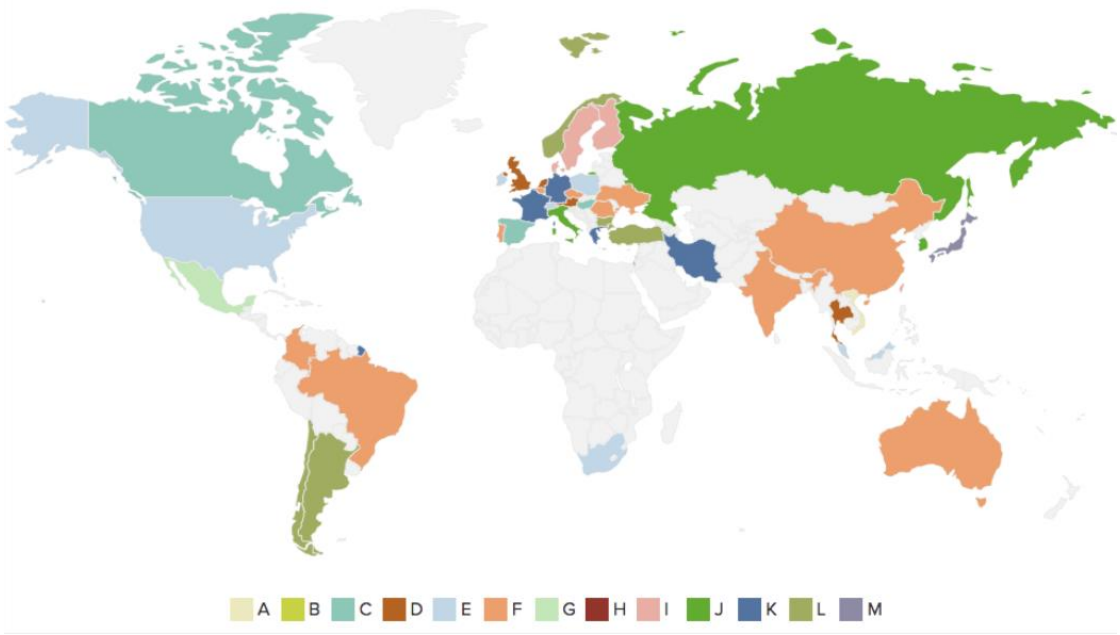
# Mô hình Master-Slave

- Trong mô hình Master-Slave:
  - Máy chủ Master là máy chủ trực tiếp quản lý các bản ghi tài nguyên, các công tác thêm/xóa/thay đổi bản ghi tài nguyên thực hiện trên máy máy chủ DNS Master. Máy chủ Master thực hiện đồng bộ dữ liệu zone tên miền (file dữ liệu) cho máy chủ Slave.
  - Máy chủ Slave là máy chủ nhận đồng bộ dữ liệu zone tên miền từ máy chủ Master.
  - Qúa trình đồng bộ dữ liệu từ máy chủ Master đến máy chủ Slave được gọi là zone transfer.
  - Có 1 máy chủ Master và nhiều máy chủ Slave
  - Một máy chủ cũng có thể vừa đóng vai trò là máy chủ Master đối với máy chủ này và là máy chủ Slave với máy chủ khác.



# Máy chủ Root

- Máy chủ Root là máy chủ tên miền quản lý zone tên miền Root.
- Có 13 cụm máy chủ Root, danh sách, số lượng, vị trí máy chủ từng cụm Root chi tiết tại địa chỉ: https://root-servers.org/.
- File dữ liệu của zone Root được công khai tại địa chỉ: https://www.iana.org/domains/root/files
- Tại Việt Nam, hiện đang đặt 5 máy chủ Root thuộc 3 cụm máy chủ K, F, M.



# 13 cụm máy chủ Root (1/2)

- DNS Root Zone – Hints File

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Dec 12, 2008
;       related version of root zone:   2008121200
;
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
;
;
FORMERLY C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; FORMERLY NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
H.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:1::803F:235
```

# 13 cụm máy chủ Root (2/2)

- DNS Root Zone – Hints File

```
FORMERLY NIC.NORDU.NET
;
.                    3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
;
; OPERATED BY VERISIGN, INC.
;
.                    3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.                    3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.      3600000      AAAA  2001:7FD::1
;
; OPERATED BY ICANN
;
.                    3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:3::42
;
; OPERATED BY WIDE
;
.                    3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.      3600000      AAAA  2001:DC3::35
; End of File
```

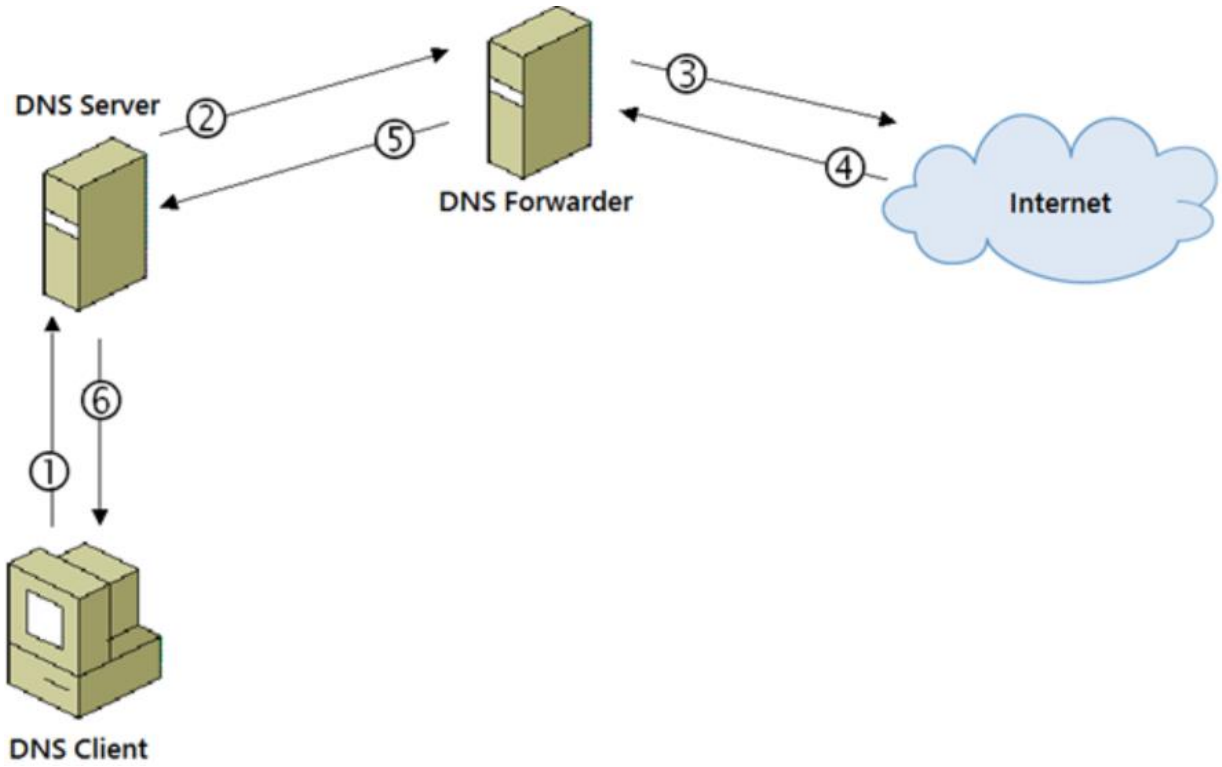
# DNS Cache (1/2)

- DNS Cache hay còn gọi là Caching Recursive Resolver
- DNS Cache không được chuyển giao tên miền nào, không quản lý tên miền nào
- DNS Cache là máy chủ thực hiện chức năng như Resolver tạo ra các yêu cầu truy vấn Recursive (truy vấn đệ quy), gửi truy vấn tên miền gửi đến các máy chủ tên miền theo thứ tự chuyển giao để tìm ra câu trả lời cuối cùng, lưu thông tin vào máy chủ trong 1 khoảng thời gian (được gọi là lưu Cache).
- Tinh năng lưu Cache được hiểu rằng các thông tin về câu trả lời nhận được từ các máy chủ tên miền sẽ được lưu lại trong một khoảng thời gian, thời gian này theo giá trị TTL của từng bản ghi tài nguyên tương ứng, giúp cho hoạt động truy vấn tên miền nhanh chóng, giảm tải cho các máy chủ.

# DNS Cache (2/2)

- Nếu có truy vấn tên miền bản ghi RR được gửi đến DNS Cache
  - Trong thời gian TTL của bản ghi RR, thông tin bản ghi RR vẫn còn lưu trên DNS Cache, DNS Cache lấy luôn thông tin bản ghi RR đang lưu để trả lời cho Client.
  - Sau thời gian TTL, máy chủ DNS Cache sẽ thực hiện truy vấn để tìm thông tin trả lời, sau đó tiếp tục lưu Cache theo giá trị TTL.
- Nếu giá trị TTL của bản ghi tài nguyên nhỏ, dữ liệu sẽ được cập nhật thường xuyên, sẽ được đảm bảo tính chính xác, tuy nhiên các máy chủ tên miền và DNS Cache sẽ phải chịu tải nhiều hơn.
- Nếu giá trị TTL của bản ghi tài nguyên lớn, dữ liệu không thường xuyên được cập nhật có thể không đảm bảo tính chính xác của bản ghi.

# DNS Forwarder




- DNS Forwarder là máy chủ thực hiện chức năng tiếp nhận chuyển tiếp truy vấn tên miền

Tính năng chuyển tiếp truy vấn tên miền này có thể thực hiện:

- Chuyển tiếp tất cả các truy vấn tên miền hoặc tên miền cụ thể.
- Chỉ thực hiện chuyển tiếp truy vấn tên miền mà không thực hiện phân giải tên miền.
- Thực hiện chuyển tiếp truy vấn tên miền trước, nếu máy chủ được chuyển tiếp truy vấn không thực hiện phân giải được, thì sau đó máy chủ sẽ thực hiện tìm câu trả lời trong bộ nhớ Cache.

# DNS Hybrid

- DNS Hybrid là máy chủ hỗn hợp, máy chủ thực hiện nhiều chức năng của các loại máy chủ.
- Ví dụ về máy chủ DNS Hybrid:
  - Máy chủ thực hiện đồng thời 02 chức năng là quản lý tên miền của máy chủ Authoritative và chức năng thực hiện truy vấn tên miền theo cơ chế Recursive (truy vấn đệ quy), lưu Cache thì là một máy chủ DNS Hybrid.
  - Máy chủ thực hiện đồng thời 02 chức năng là quản lý tên miền của máy chủ Authoritative và chức năng thực chuyển tiếp tên miền.

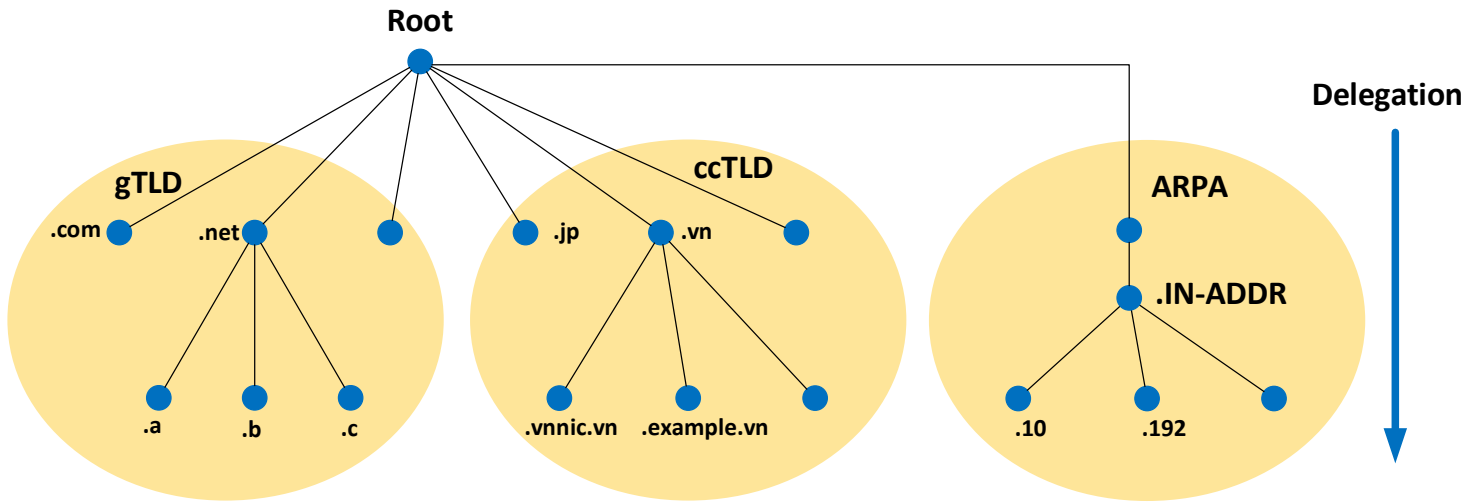
# III. Nguyên lý hoạt động

# Nguyên lý hoạt động của DNS

- Chuyển giao (Delegation)
- Đồng bộ dữ liệu
  - Đồng bộ toàn phần (AXFR)
  - Đồng bộ một phần (IXFR)
- Ánh xạ tên miền
- Truy vấn tên miền
  - Truy vấn đệ quy
  - Truy vấn không đệ quy
- Phân giải tên miền

# Chuyển giao (Delegation) (1/2)

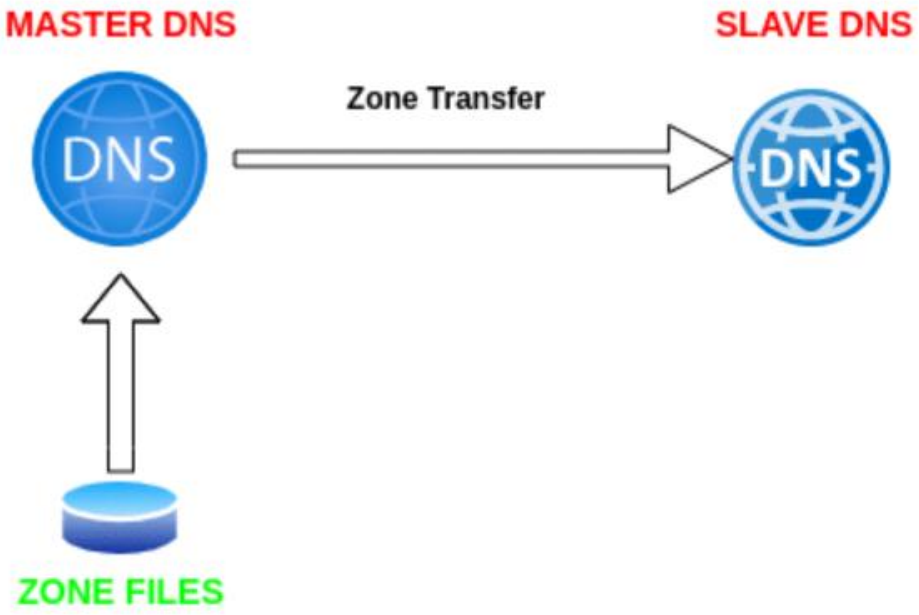
- Hệ thống tên miền mới được xây dựng trên cấu trúc quản lý không tập trung, được xây dựng dựa trên quá trình chuyển giao.
- Quá trình chuyển giao là quá trình thực hiện chia một domain này thành các subdomain và giao cho các tổ chức khác nhau quản lý subdomain này.
- Khi thực hiện quá trình chuyển giao, tổ chức được chuyển giao tên miền sẽ có toàn quyền quản lý với subdomain mà mình được chuyển giao về.
- Người quản trị có thể tạo ra miền con (subdomain) và tiếp tục chuyển giao.

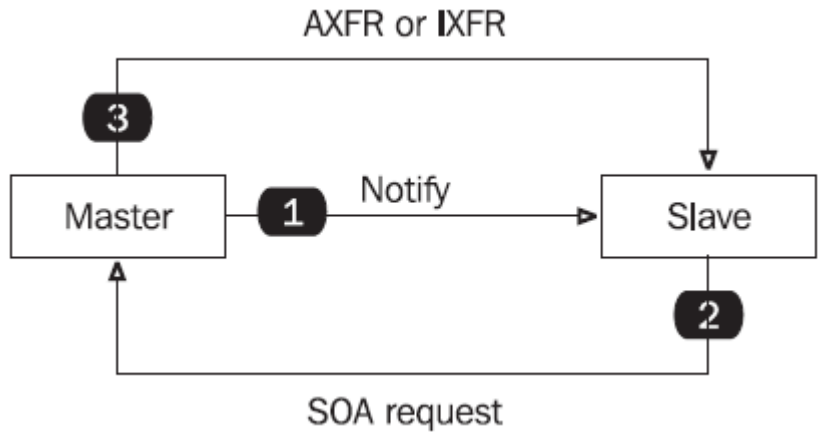


# Chuyển giao (Delegation) (2/2)

- Ví dụ:
  - Một tổ chức có tên miền example.com.vn
  - Chia thành các subdomain: sub1, sub2, sub3 dưới example.com.vn
  - Chuyển giao các sub này cho các đơn vị khác quản lý, có thể phân chia theo vùng địa lý, phân cấp tổ chức, phân cấp dịch vụ ….
  - Tổ chức được chuyển giao tên miền có thể khai báo các tên miền cấp dưới tên được chuyển giao: www.sub1.example.com, có thể tiếp tục chuyển giao tên miền được phân cấp.

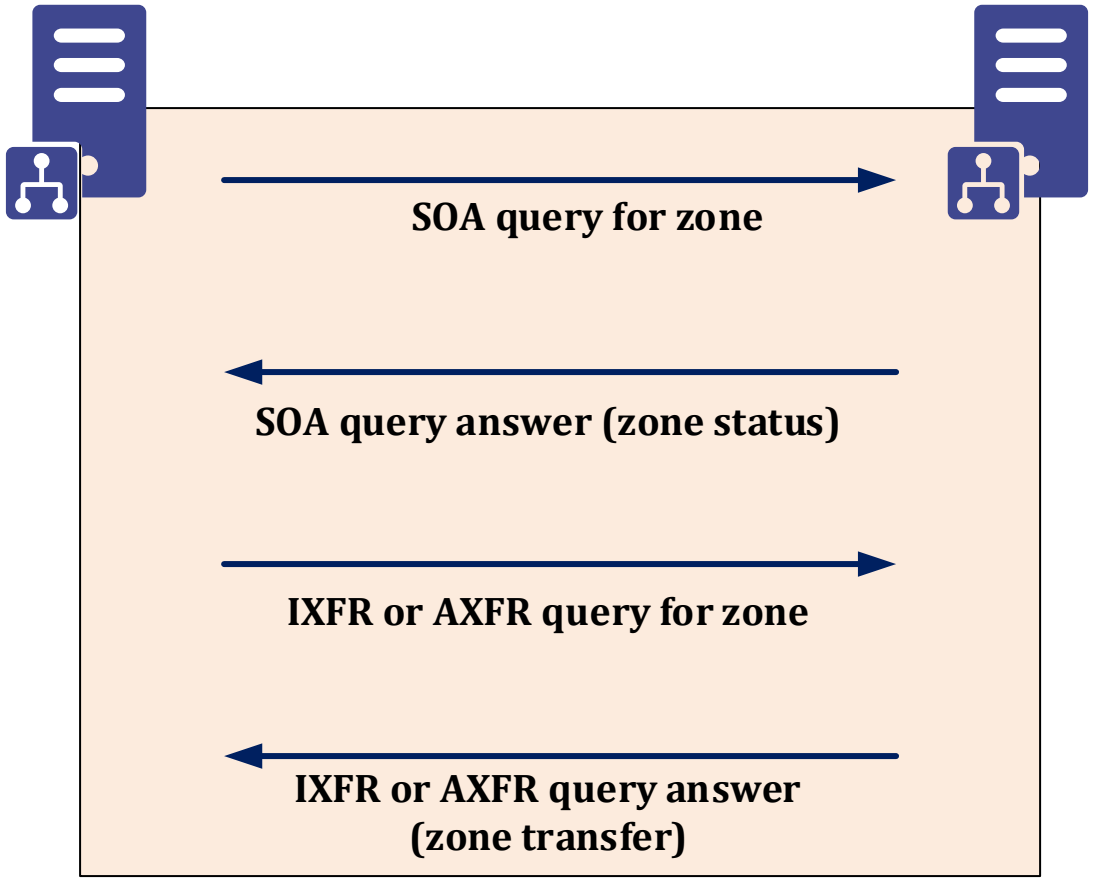
# Đồng bộ dữ liệu (1/2)




- Qúa trình đồng bộ dữ liệu từ máy chủ Master đến máy chủ Slave được gọi là zone transfer, sử dụng giao thức TCP, port 53.
- Mặc định gửi đến tất cả các máy chủ khai báo trong bản ghi NS của zone.
- Sử dụng thông tin Serial trong bản ghi SOA để xác định việc thực hiện đồng bộ dữ liệu.
- Serial thường đặt theo định dạng yyyymmddss (thứ tự là năm tháng ngày số lần thay đổi)
- Sau khi máy chủ Master thay đổi dữ liệu cần tăng giá trị Serial để đảm bảo việc đồng bộ dữ liệu đến các máy chủ Slave
- Có 02 hình thức đồng bộ:
  - Đồng bộ toàn bộ dữ liệu theo giao thức AXFR (Full Zone Transfer)
  - Đồng bộ dữ liệu thay đổi theo giao thức IXFR (Incremental Zone Transfer)
  - RFC1996

# Đồng bộ dữ liệu (2/2)




- Qúa trình zone transfer thực hiện trong 03 trường hợp sau:
  - Định kỳ theo giá trị Refresh trong bản ghi SOA của zone tên miền, máy chủ Slave sẽ gửi yêu cầu truy vấn bản ghi SOA của máy chủ Master để lấy thông tin Serial và so sánh với giá trị đang có, nếu giá trị thấp hơn thực hiện gửi yêu cầu zone transfer đến máy chủ Master.
  - Khi máy chủ Master thực hiện cập nhật dữ liệu sẽ gửi thông báo (gọi là notify) đến các máy chủ tên miền nằm trong danh sách bản ghi NS của tên miền hoặc theo cấu hình cụ thể, lúc này máy chủ Slave thực hiện gửi yêu cầu zone transfer dữ liệu đến máy chủ Master.
  - Một trong 02 loại máy chủ thực hiện khởi động lại dịch vụ tên miền, nếu là máy chủ Slave thì sẽ gửi yêu cầu đồng bộ đến máy chủ Master, nếu là máy chủ Master thì đồng bộ đến các máy chủ Slave.

# Đồng bộ toàn phần (AXFR)

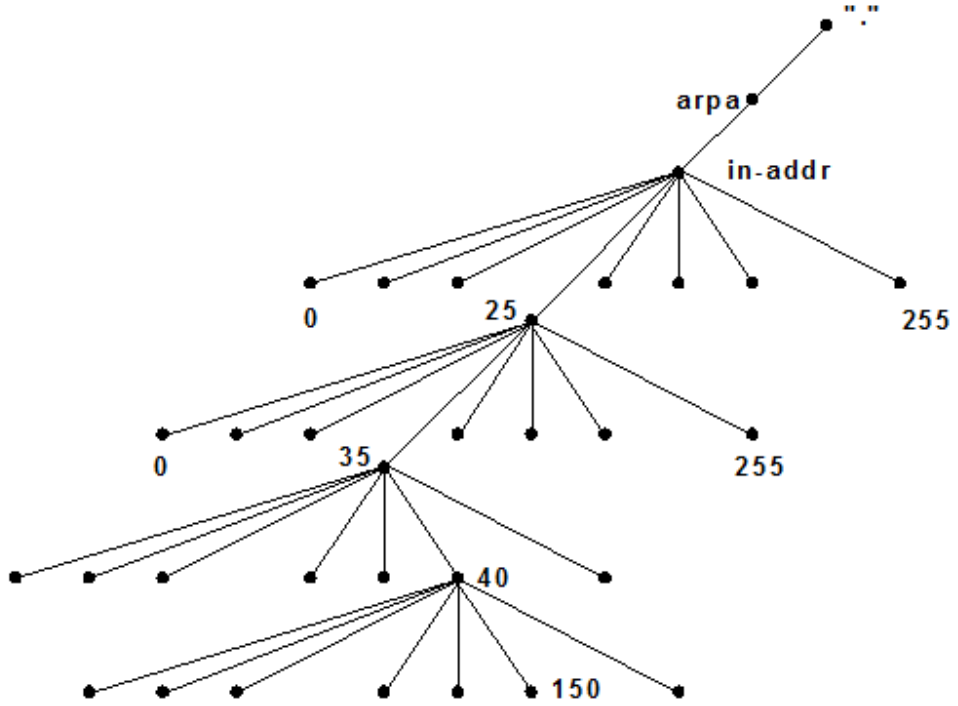
- Full Zone Transfer (AXFR): đề cập trong RFC 1034 và 1035, Slave của một zone phải lấy dữ liệu (pull) của zone từ Master.
- Thời gian giữa 02 lần pull xác định bởi giá trị của trường refresh trong bản ghi SOA của zone đó.
  - Slave truy vấn bản ghi SOA của máy chủ Master
  - Nếu trường Serial của Master lớn hơn giá trị hiện tại của Slave thì Slave sẽ gửi yêu cầu AXFR đến Master để cung cấp toàn bộ dữ liệu thông tin của Zone.
  - Phải thay đổi serial number khi thay đổi dữ liệu của Zone trên máy Master.
- Zone transfer (AXFR) sử dụng TCP, port 53.

# Đồng bộ một phần (IXFR)

- Incremental Zone Transfer (IXFR) đề cập trong RFC 1995:
  - Hữu ích khi chỉ có một số ít RR được thay đổi  trên Master
  - Khắc phục việc thực hiện AXFR gây lãng phí băng thông và thời gian đồng bộ
  - Song song cùng hoạt động với AXFR
- Hoạt động tương tự AXFR
  - Truy vấn bản ghi SOA theo thời gian xác định bởi Serial number trong SOA
  - Gửi yêu cầu đồng bộ, kèm theo cờ chỉ ra rằng nó hỗ trợ IXFR,
  - Nếu Master hỗ trợ thì  thực hiện IXFR
  - Nếu Master không hỗ trợ thì thực hiện AXFR
- IXFR sử dụng TCP port 53

# Ánh xạ tên miền

- Ánh xạ thuận: Forward mapping
  - Chuyển đổi tên miền sang địa chỉ
- Ánh xạ ngược: Reverse Mapping
  - Chuyển đổi địa chỉ sang tên miền
  - Phân cấp tên miền dưới nhánh in-addr.arpa
  - Domain in-addr.arpa sẽ gồm có 4 cấp,
  - Mỗi cấp sẽ có 256 domain
  - Tương ứng với 256 cách đánh địa chỉ ở mỗi octet.

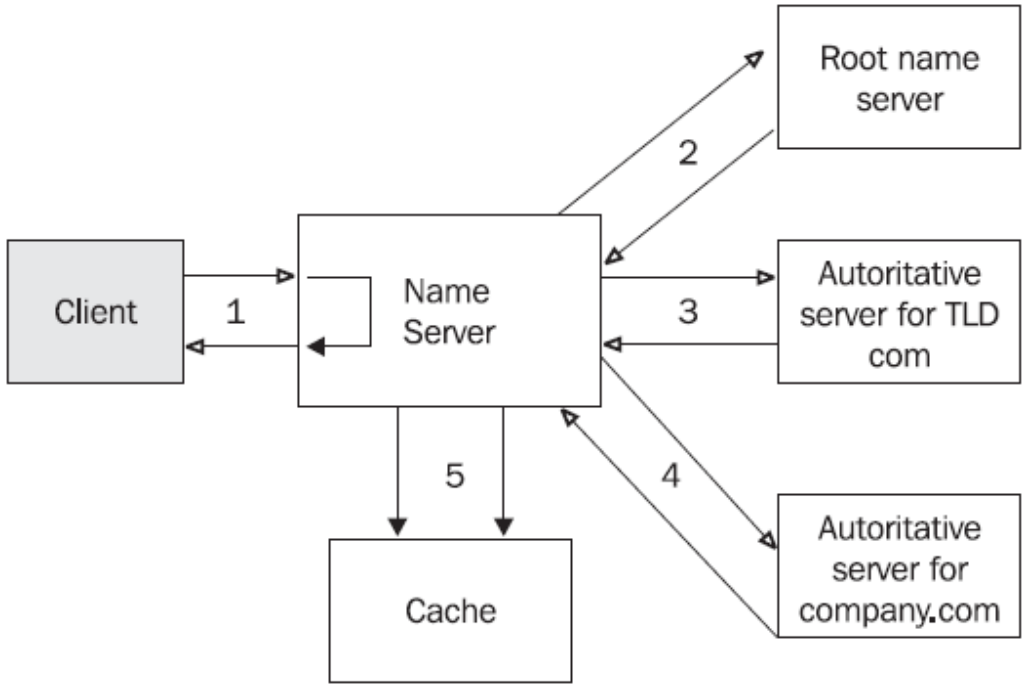


# Truy vấn tên miền (1/2)

- Truy vấn tên miền là quá trình tìm kiếm thông tin liên quan đến một tên miền cụ thể trong hệ thống phân giải tên miền.
- Truy vấn tên miền được thực hiện để xác định thông tin tương ứng với tên miền đó, thông tin có thể là địa chỉ IP, máy chủ Mail, máy chủ tên miền, ….
- Truy vấn tên miền là việc Client thực hiện các yêu cầu thông tin tên miền (gửi các câu hỏi về tên miền) đến các máy chủ.
- Phân giải tên miền là quá trình nhận được truy vấn tên miền, thực hiện tìm kiếm thông tin và trả về Client

# Truy vấn tên miền (2/2)

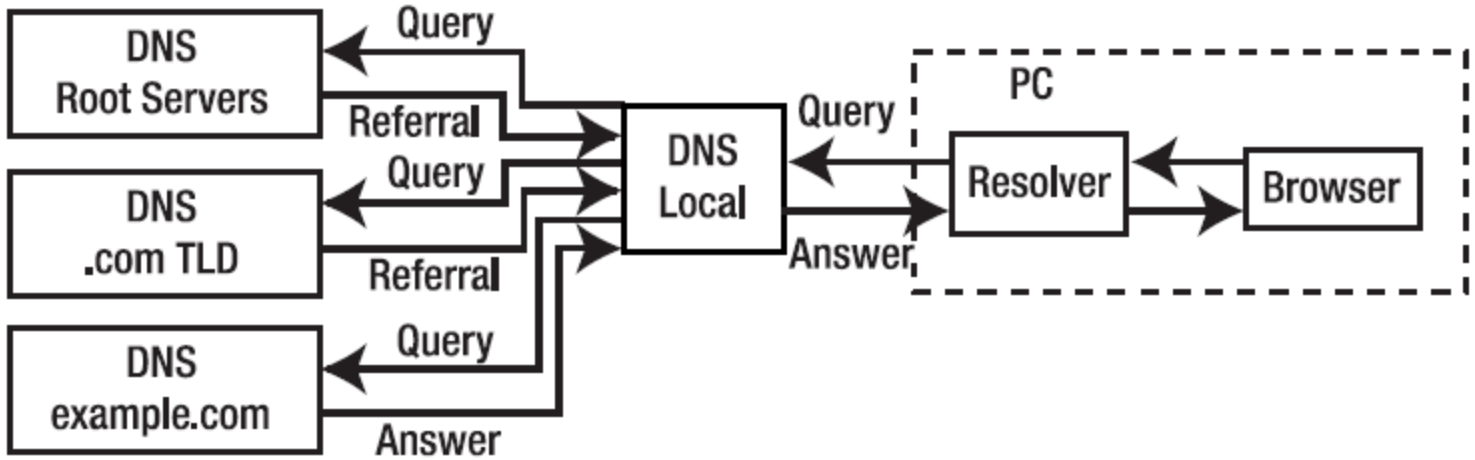
- Truy vấn theo cơ chế phân cấp tên miền và hệ thống DNS
- DNS trực tiếp quản lý tên miền (Authoritative) sẽ có câu trả lời về tên miền được truy vấn.
- Quá trình truy vấn tiêu chuẩn gồm 5 (4 bước phân giải và 1 bước lưu Cache) bước như hình bên:



# Truy vấn đệ quy

- Truy vấn đệ quy (Recursive) là truy vấn yêu cầu phải thực hiện tạo truy vấn tên miền đến tất cả các máy chủ theo thứ tự chuyên giao tên miền từ máy chủ Root đến máy chủ quản lý tên miền để tìm ra được câu trả lời cuối cùng.

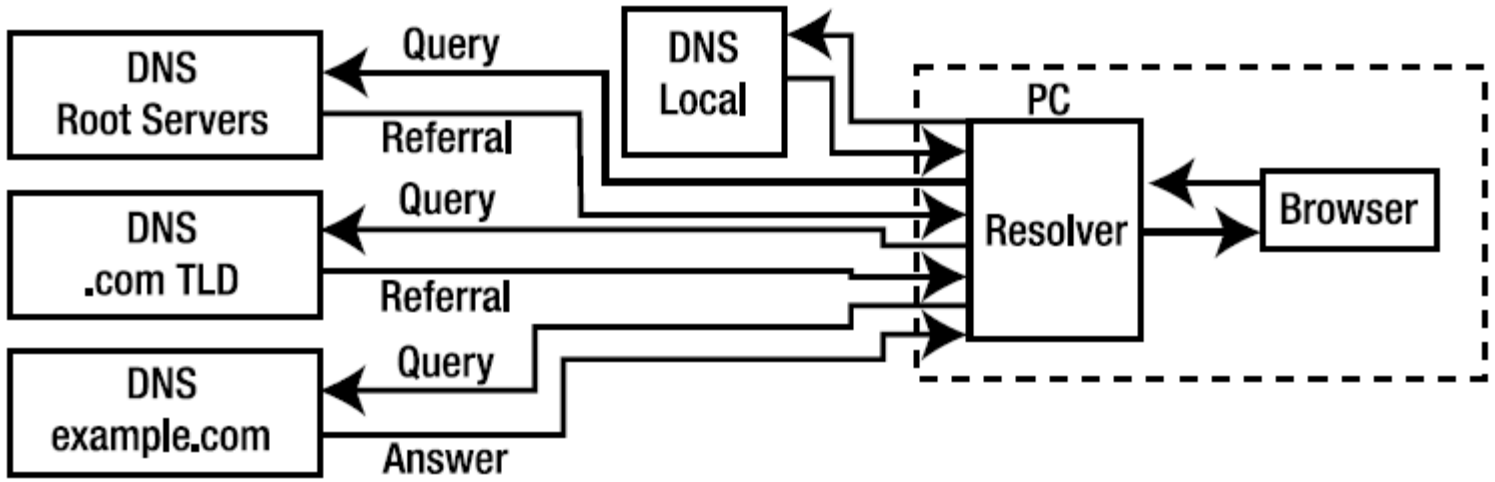
- Truy vấn gửi đến máy chủ DNS Cache thông thường là truy vấn đệ quy.



# Truy vấn không đệ quy

- Truy vấn không đệ quy (Non-Recursive) là truy vấn được gửi đến máy chủ mà nếu trên máy chủ có câu trả lời thì sẽ trả lời cho Client, nếu không có câu trả lời trực tiếp thì máy chủ sẽ cung cấp thông tin cần thiết liên quan.

- Truy vấn gửi đến các máy chủ tên miền (máy chủ Authoritative) là máy chủ không đệ quy.



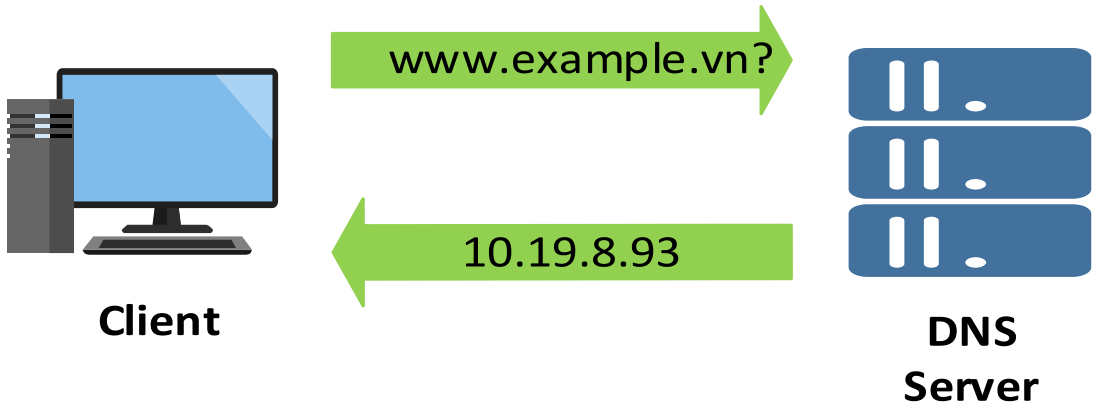
# Phân giải tên miền (1/3)

- Phân giải tên miền tên miền là ánh xạ tên miền sang địa chỉ IP hoặc các thông tin khác (ví dụ thông tin máy chủ DNS, thông tin máy chủ Mail, …)
  - IPv4:

| | | |
|---|---|---|
| **www.example.vn** | → | **10.19.8.93** |

  - IPv6:

| | | |
|---|---|---|
| **academy.vnnic.vn** | → | **2001:dce:1:2::3** |




- Và ngược lại, phân giải IP sang tên miền:
  - IPv4:

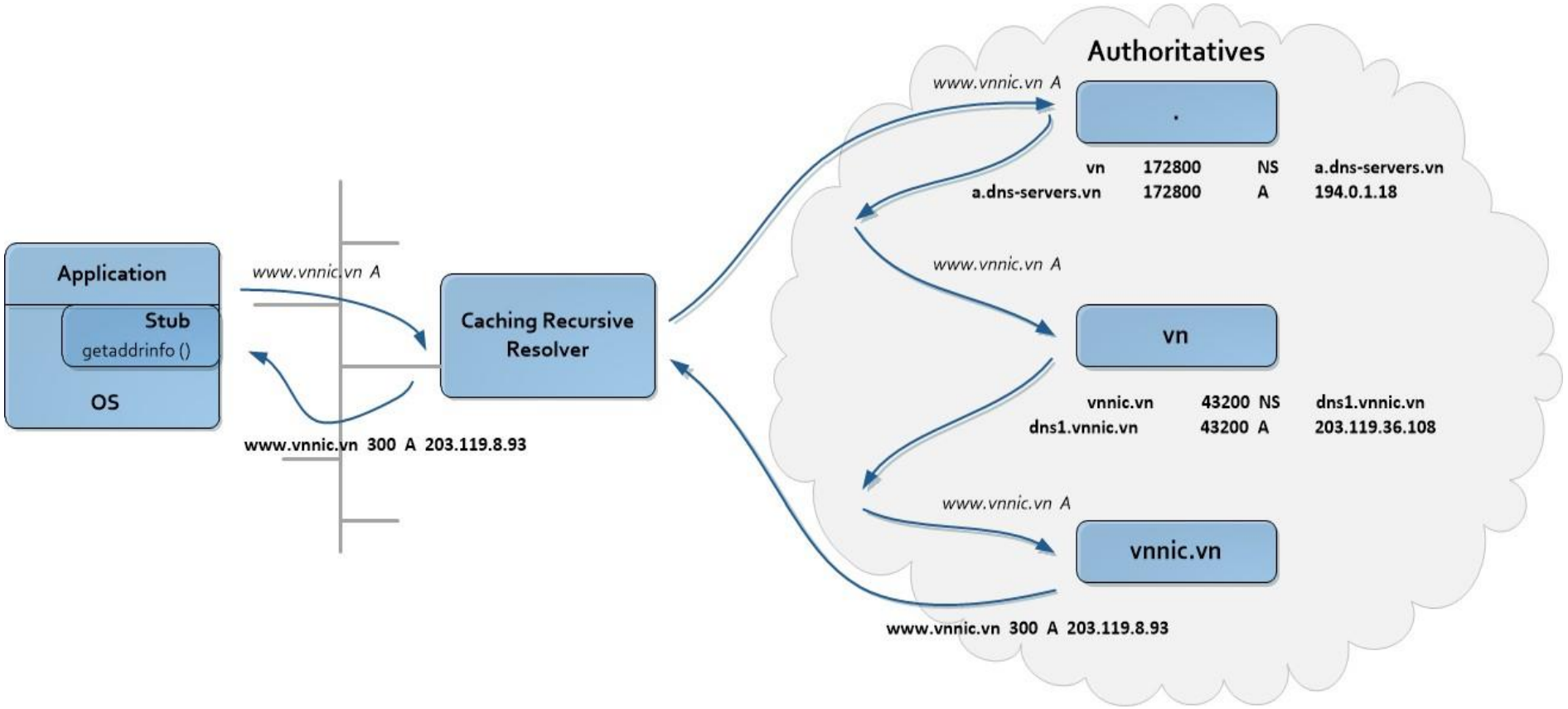
| | | |
|---|---|---|
| **93.8.19.10.in-addr.arpa** | → | **www.example.vn** |

  - IPv6:

| | | |
|---|---|---|
| **3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.1.0.0.0.e.c.d.0.1.0.0.2.ip6.arpa** | → | **academy.vnnic.vn** |

# Phân giải tên miền (2/3)

- Phân giải tên miền là quá trình nhận được truy vấn tên miền, thực hiện tìm kiếm thông tin và trả về Client.



# Công cụ

- Có một số công cụ sử dụng để truy vấn tên miền, tìm ra các thông tin của tên miền:
  - nslookup: công cụ tích hợp sẵn trên hệ điều hành của Windows
  - dig: công cụ thực hiện truy vấn tên miền, có thể cài đặt sử dụng trên Windows và Linux.
  - Công cụ online:

    https://www.menandmice.com/support/dig

    https://www.digwebinterface.com/

    https://www.diggui.com/

# IV. CÀI ĐẶT, CẤU HÌNH

# HƯỚNG DẪN CÀI ĐẶT PHẦN MỀM DNS

# Nội dung

- Hướng dẫn cài đặt phần mềm
- Hướng dẫn cấu hình dịch vụ DNS
- Hướng dẫn công tác quản trị và gỡ lỗi
- Hướng dẫn tối ưu, bảo mật

# Phần mềm DNS

- Có nhiều phần mềm DNS khác nhau: BIND, Windows DNS, CNS/ANS, NSD/Unbound, Knot, PowerDNS,...
- Môi trường cài đặt: Windows, Unix
- Phần mềm BIND là phần mềm phổ biến nhất:
  - Mã nguồn mở, miễn phí
  - Hỗ trợ Windows và Unix (Phổ biến: Unix)
  - Phát triển bởi ISC, hỗ trợ từ nhiều hãng: HP, IBM, ...
  - Năng lực xử lý cao, cấu hình mềm dẻo, an toàn.
  - Sử dụng bởi nhiều gTLD và ccTLD
- Phần mềm thương mại có bản quyền: Akamai Nominum CNS/Vantio; ANS …

# Chuẩn bị

- Tải phần mềm BIND:
  - Truy cập *http://www.isc.org*
  - Vào phần Download, chọn BIND và tải về gói .tar.gz mới nhất và ổn định nhất.
  - Sử dụng các chương trình SFTP (trong SSH), FTP để đưa gói vào máy chủ.
- Cài đặt một số công cụ, thư viện hỗ trợ cài đặt phần mềm BIND:
  - gunzip, tar, gcc, make, openssl, python, ...
- Đối với mô hình triển khai và phạm vi của các đơn vị CQNN, khuyến nghị cấu hình tối thiểu môi trường cài đặt như sau:
  - Máy chủ ảo hóa; CPU: 1 vCPU, 1.8 GHz (share); HDD: 200 GB; RAM: 8 GB; Ethernet: 1 Gbps (share)
  - HĐH: Unix 7.0

# Hướng dẫn cài đặt phần mềm DNS

- Giải nén
- Cài đặt phần mềm BIND
- Kiểm tra

# Giải nén

- Thực hiện lệnh: # tar –xvf  bind-9.11.17-P1.tar.gz
- File sẽ được giải nén tại thư mục bind-9.11.17-P1
- Thư mục này gồm các thư mục con:
  - Bin: Chứa các mã nguồn của chương trình BIND
  - Contrib: Chứa các công cụ, phần mềm để sử dụng với phần mềm BIND
  - Doc: Chứa tài liệu hướng dẫn
  - Lib: Chứa các mã nguồn của thư viện dùng cho phần mềm BIND
  - Make: Chứa các file để biên dịch và cài đặt chương trình.

# Cài đặt

- Thực hiện các lệnh sau theo thứ tự để cài đặt phần mềm BIND:
  - *# ./configure +[Options] (ví dụ: --prefix=/opt/mydns/bind910/bind-9.10.1-P1/linux/bind9101p1, --enable-largefile, --enable-fixed-rrset, --enable-filter-aaaa, --enable-threads , --with-openssl=$openssl_dir, --with-gssapi=$krb_dir, --with-libxml2=$libxml2_dir, …)*
  - *# make all*
  - *# make install*
- Mặc định các file chương trình của phần mềm BIND sẽ được cài tại thư mục:
  - *# /usr/local/sbin và /usr/local/bin*

# Kiểm tra

- Kiểm tra BIND phiên bản phần mềm BIND:
  - *# /usr/local/sbin/named –v*
  - *# named –v*

    BIND 9.11.17-P1
- Kiểm tra các file cài đặt
  - *# ls /usr/local/sbin*

  dnssec-keygen, dnssec-makekeyset, dnssec-signkey, dnssecsignzone, lwresd, named-checkconf, named-checkzone, rndc, rndc-confgen, named, …
  - *# ls /usr/local/bin*

  dig, host, isc-config.sh, nslookup, nsupdate

# HƯỚNG DẪN CẤU HÌNH DỊCH VỤ DNS

# Hướng dẫn cấu hình dịch vụ

- Thiết lập File cấu hình
- Thiết lập File dữ liệu
- Thiết lập hoạt động Master-Slave
- Thiết lập DNS Cache

# Hướng dẫn cấu hình dịch vụ

- Dịch vụ BIND hoạt động cần có file cấu hình và file dữ liệu
- File cấu hình thông thường là /etc/named.conf
- File dữ liệu được chỉ ra trong file cấu hình, thông thường /var/named/
- Khi khởi động, phần mềm BIND đọc file cấu hình và các file dữ liệu tương ứng.
- Các bước thực hiện:
  - Soạn file cấu hình (named.conf)
  - Soạn file dữ liệu zone (zone file)
  - Kiểm tra cấu trúc của file cấu hình và file dữ liệu
  - Chạy chương trình DNS (named)

# Thiết lập file cấu hình

- **File cấu hình: named.conf**
  - Ví dụ

```
options {
        directory "/var/named";
};
controls {
        inet 127.0.0.1 allow { localhost; }
        keys {rndckey; };
};
include "/etc/rndc.key";
zone "." IN {
        type hint;
        file "named.root";
};
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};
zone "example.vn" {
        type master;
        file "example.vn.db";
        notify yes;
};
```

# Thiết lập File dữ liệu

- **File dữ liệu:**
  - Ví dụ:

```
$TTL 7200
example.vn.          IN    SOA    dns1.example.vn. dnsadmin.example.vn. (
                                  2020101501 ; Serial
                                  3600 ; Refresh 1 hours
                                  1800 ; Retry 30 minutes
                                  604800 ; Expire 1 week
                                  7200 ; Negative cache 2 hours
                                  )
                     IN    NS     dns1.example.vn.
                     IN    NS     dns2.example.vn.
$ORIGIN example.vn.
www                  IN    A      10.10.2.10
home                 IN    CNAME  www
```

# Thiết lập hoạt động Master-Slave

- Trên máy chủ DNS Master cho phép thực hiện đồng bộ dữ liệu.
  - allow-transfer {IP của máy chủ Slave};
- Trên máy chủ DNS Slave thiết lập thông tin máy chủ DNS Master của zone tên miền
  - masters {IP của máy chủ Master};

# Thiết lập DNS Cache

- Không quản lý tên miền nào
- Thực hiện truy vấn đệ quy
- Sử dụng “type hint”

```
options {
        directory "/etc/named";
};
//root name servers – hint zone
zone "." {
        type hint;
        file "root.hint";
};
//reverse mapping for 127.0.0.1
zone "0.0.127.in-addr.arpa"{
        type master;
        file “named.lcoal";
        notify no;
};
```

# CÔNG TÁC QUẢN TRỊ VÀ GỠ LỖI

# Nội dung

- Hướng dẫn kiểm tra, chỉnh sửa file cấu hình
- Hướng dẫn kiểm tra, chỉnh sửa file dữ liệu
- Hướng dẫn bật/tắt/khởi động dịch vụ
- Thiết lập ghi nhật ký dịch vụ phục vụ công tác quản trị, vận hành, gỡ lỗi
- Thiết lập RNDC
- Các công cụ gỡ lỗi

# Kiểm tra, sửa File cấu hình

- Kiểm tra cấu hình **named.conf** sử dụng lệnh: named-checkconf
  - *# /usr/local/sbin/named-checkconf /etc/named.conf*
- Trong trường hợp không có lỗi, chương trình sẽ không thông báo gì
- Trường hợp có lỗi, chương trình sẽ thông báo lỗi và vị trí lỗi.
- Dựa trên thông báo, chỉnh sửa lại cấu hình cho phù hợp.
- Sau khi sửa xong và lưu file, sau đó thực hiện kiểm tra file cấu hình để đảm bảo cú pháp và nội dung file đã đúng.

# Kiểm tra, sửa File dữ liệu

- Kiểm tra file dữ liệu:
  - *# named-checkzone “zonename” “filename”*
- Trong trường hợp file dữ liệu có lỗi cú pháp, chương trình sẽ thông báo lỗi gặp phải.
- Dựa trên thông báo, điều chỉnh lại cấu hình cho phù hợp.
- Tương tự như quá trình kiểm tra lỗi của file cấu hình, sau khi kiểm tra và sửa lỗi xong, tiến hành chạy lệnh named-checkzone để kiểm tra lại một lần nữa nhằm đảm bảo cú pháp đã được sửa đúng.
- Ví dụ:
  - *# named-checkzone example.vn /var/named/example.vn.db*

  zone example.vn/IN: loaded serial 2009080800 OK

# Bật dịch vụ DNS

- Khi cài đặt phần mềm Bind, chương trình named được đặt tại thư mục /usr/local/sbin và file named.conf được đặt tại thư mục /etc, để chạy chương trình named thực hiện lệnh sau:

  - *# /usr/local/sbin/named –c /etc/named.conf*

  - Kiểm tra tiến trình PID (Process Identifier: Định danh tiến trình) đang chạy:

  - *# ps -ef | grep named*

    root 12640 1 0 22:59 ? 00:00:00 named

  → Như thông báo trên chương trình named đang chạy với Process ID (PID) là 12640.

# Tắt/ khởi động lại dịch vụ DNS

- Tắt dịch vụ DNS thực hiện lệnh:
  - *# kill -9 PID (Process ID)*
- Khởi động lại dịch vụ DNS thực hiện lệnh:
  - *# kill –HUP PID*

# Nhật ký dịch vụ DNS trên hệ thống

- Mặc định nhật ký hoạt động của named sẽ đưa vào syslog của hệ thống
  - */var/log/message*
- Xem log:
  - *# tail –f /var/log/message*

# Kiểm tra dịch vụ DNS

- Kiểm tra hoạt động của named:
  - *# ps –ef | grep named*
- Nếu chương trình named đã hoạt động, nhận được kết quả Process ID của chương trình named:
  - *# ps -ef | grep named*

  root 12640 1 0 22:59 ? 00:00:00 named
- Kiểm tra file cấu hình, file dữ liệu:
  - File cấu hình: named-checkconf
  - File dữ liệu: named-checkzone

# RNDC (1/2)

- rndc (**r**emote **n**ame **s**erver **c**ontrol) là công cụ cho phép điều khiển BIND từ xa, đảm bảo an toàn thông qua việc sử dụng key.
- Chương trình tương tác với BIND qua các tín hiệu signal
- Phiên làm việc được mã hóa bằng khóa đối xứng.
  - BIND: lưu khóa trong named.conf
  - RNDC: lưu khóa trong rndc.conf hoặc rndc.key
- Tạo khóa bằng công cụ rndc-confgen –a
- Thực hiện lệnh:
  - *# rndc [-c config][-s server][-p port][-key] command*

# RNDC (2/2)

**File rndc.key**

```
key "rndc-key" {
    algorithm hmac-md5;
    secret
    "WjaYvvX40PPmL0dzv8Tsn
    A==";
};
```

**File named.conf**

```
key "rndc-key" {
    algorithm hmac-md5;
    secret
    "WjaYvvX40PPmL0dzv8Tsn
    A==";
};

controls {
inet 194.17.165.23 port 953
    allow { 194.17.165.23;
    194.17.14.148; }
 keys {"rndc-key";};
};
```

# NSLOOKUP

- Là một tiện ích tra cứu tên miền, được tích hợp sẵn trong hệ điều hành Windows, Unnix

```
C:\>nslookup
> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> set type=a
> tinhte.vn
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    tinhte.vn
Addresses:  125.212.247.5
          125.212.247.8
```

```
C:\>nslookup
> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> set type=ns
> tinhte.vn
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
tinhte.vn       nameserver = donald.ns.cloudflare.com
tinhte.vn       nameserver = lisa.ns.cloudflare.com
```

# DIG (1/3)

- **DIG** (**D**omain **I**nformation **G**roper)
- Công cụ tra cứu, chuẩn đoán DNS.
- Kèm theo phần mềm BIND.
- Trên Windows dig không đọc được thông tin cấu hình resolver trong Registry.
  - Cần thêm: nameserver [DNS_IP] vào file
  - %SystemRoot%\system32\drivers\etc\resolv.conf
- Cung cấp rất nhiều tùy chọn

# DIG (2/3)

- Cú pháp của lệnh: dig [@dns] domain [[-c ]q-type]
  - [@dns]: Tên hoặc địa chỉ IP của máy chủ DNS
  - Domain: Xác định tên miền đang query
  - Type: Tìm kiếm với các kiểu bản ghi nào Any, SOA, A, AAAA, NS, MX…
- Ví dụ:
  - dig @8.8.8.8 www.tinhte.vn A

```
; <<>> DiG 9.11.23 <<>> @8.8.8.8 www.tinhte.vn A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30011
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.tinhte.vn.                 IN      A

;; ANSWER SECTION:
www.tinhte.vn.          208     IN      A       125.212.247.5
www.tinhte.vn.          208     IN      A       125.212.247.8

;; Query time: 25 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Oct 15 14:11:59 SE Asia Standard Time 2020
;; MSG SIZE  rcvd: 74
```

# DIG (3/3)

- Các công cụ có trên web:
  - https://www.diggui.com/
  - https://www.menandmice.com/support/dig/
  - http://www.dnsstuff.com/
  - http://www.kloth.net/
- Ứng dụng trên điện thoại:
  - ISC Dig: https://apps.apple.com/vn/app/isc-dig/id1115648880?l=vi

# Nhật ký hoạt động (Log) (1/3)

- Hỗ trợ việc quản lý, giám sát hoạt động.
- Mặc định BIND ghi log vào log hệ thống tại file: /var/log/message.
  - Xem thông tin về hoạt động của BIND: *# tail –f /var/log/messages*
- BIND cho phép cấu hình thay đổi việc ghi nhật ký, thực hiện cấu hình ghi nhật ký trong file cấu hình: /etc/named.conf
- Chi tiết tham khảo Administrator's Reference Manual (ARM)

# Nhật ký hoạt động (Log) (2/3)

- **default**: log mặc định bao gồm các loại không được chỉ định rõ trong phần statement.
- **general**: bao gồm các loại không được chỉ định rõ.
- **client**: xử lý yêu cầu của client.
- **config**: phân tích file cấu hình và xử lý.
- **database**: liên quan đến cấu trúc bên trong của BIND, được sử dụng để lưu dữ liệu zone và bộ nhớ đệm các bản ghi.
- **dnssec**: xử lý DNSSEC
- **lame-servers**: phát hiện chuyển giao bị lỗi.
- **network:** hoạt động của mạng
- **notify:** thông báo thay đổi của zone theo cơ chế Asyn
- **queries:** log truy vấn
- **resolver:** phân giải tên miền, bao gồm truy vấn đệ quy từ resolvers
- **security:** chấp nhận/không chấp nhận yêu cầu
- **update:** sự kiện cập nhật động
- **update-security:** không chấp nhận/chấp nhận cập nhật động
- **xfer-in:** thông tin zone transfer nhận được máy chủ khác
- **xfer-out:** thông tin zone transfer gửi đến máy chủ khác

# Nhật ký hoạt động (Log) (3/3)

- **Ví dụ:**

```
logging{
channel simple_log {
        file        "/var/log/named/bind.log“
versions 3 size 5m;
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;
};
category default{ simple_log;};
```

```
logging {
channel "test_channel" {
        file "test.log“ versions 4;
        print-time yes;
        print-category yes;
        print-severity yes;
        severity warning;
};
category default { test_channel;};
};
```

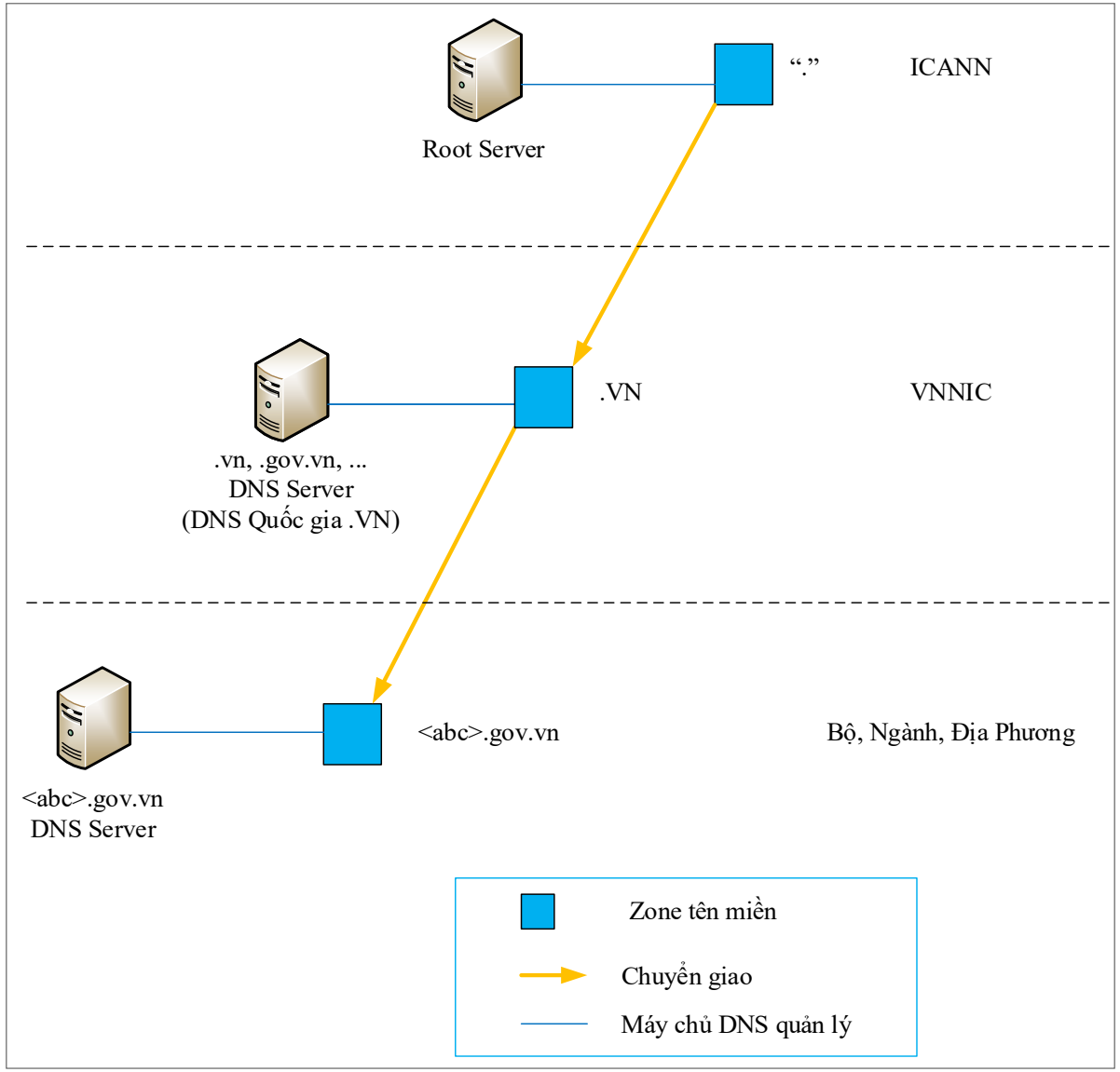
# V. MÔ HÌNH TIÊU CHUẨN HỆ THỐNG DNS CHO CQNN, TỔ CHỨC, DOANH NGHIỆP

# Nội dung

- Phân cấp tên miền và máy chủ DNS quản lý tên miền VN
- Những vấn đề cơ bản đối với hệ thống DNS
- Hiện trạng hệ thống DNS
- Sự cần thiết thiết có hệ thống DNS riêng
- Mô hình tiêu chuẩn và khuyến nghị hệ thống DNS Authoritative
- Mô hình tiêu chuẩn và khuyến nghị hệ thống DNS Cache

# Phân cấp tên miền và máy chủ DNS quản lý tên miền VN

- ICANN phân cấp, chuyển giao tên miền mã quốc gia cho các quốc gia quản lý. VD: tên miền .VN, GOV.VN, … cho Việt Nam (VNNIC) quản lý.
- Quốc gia phân cấp các tên miền cấp dưới cho các tổ chức quản lý. VD: tên miền <ABC>.gov.vn được phân cấp cho 1 Bộ/Ngành/Địa phương quản lý.
- Bộ/Nghành/Địa phương thiết lập hệ thống DNS để quản lý tên miền <ABC>.gov.vn được phân cấp.



# Những vấn đề cơ bản đối với hệ thống DNS

- Mô hình chưa chuẩn hóa, chưa đảm bảo an toàn và chưa có dự phòng.
- Chưa triển khai DNS hoạt động IPv6.
- Sử dụng phần mềm không đảm bảo an toàn, không thường xuyên cập nhật và vá lỗi
- Thiết lập các cấu hình kỹ thuật máy chủ DNS không đúng tiêu chuẩn, khuyến nghị
- Chưa thực hiện thiết lập các zone tên miền ngược trên các hệ thống DNS
- Chưa triển khai các giải pháp đảm bảo an toàn cho dịch vụ, đặc biệt là dịch vụ website và dịch vụ email.
- Hosting tại nước ngoài hoặc sử dụng DNS Caching nước ngoài, thiết lập chuyển tiếp (forward) đến DNS nước ngoài.

# Hiện trạng hệ thống DNS

- **Hệ thống DNS Authoritative:**
  - Có hệ thống máy chủ DNS riêng, hoặc thuê Hosting tại doanh nghiệp hoặc dịch vụ Hosting tại nước ngoài.
  - Chưa chú trọng đến thiết kế mô hình chuẩn, đảm bảo an toàn, dự phòng.
  - Chưa triển khai ký DNSSEC
  - Có nhiều điểm yếu về an toàn trong quản lý, cấu hình kỹ thuật cho máy chủ (chưa cấu hình ẩn phiên bản phần mềm DNS, cho phép đồng bộ dữ liệu ra bên ngoài, ….)
- **Hệ thống DNS Cache:**
  - Có hệ thống máy chủ riêng, tuy nhiên có nhiều điểm yếu về an toàn trong quản lý và cấu hình.
  - Sử dụng DNS Cache miền phí của nước ngoài như Google, Cloudflare, …
  - Không có hệ thống DNS Cache dự phòng hoặc sử dụng chung với hệ thống DNS Authoritative.

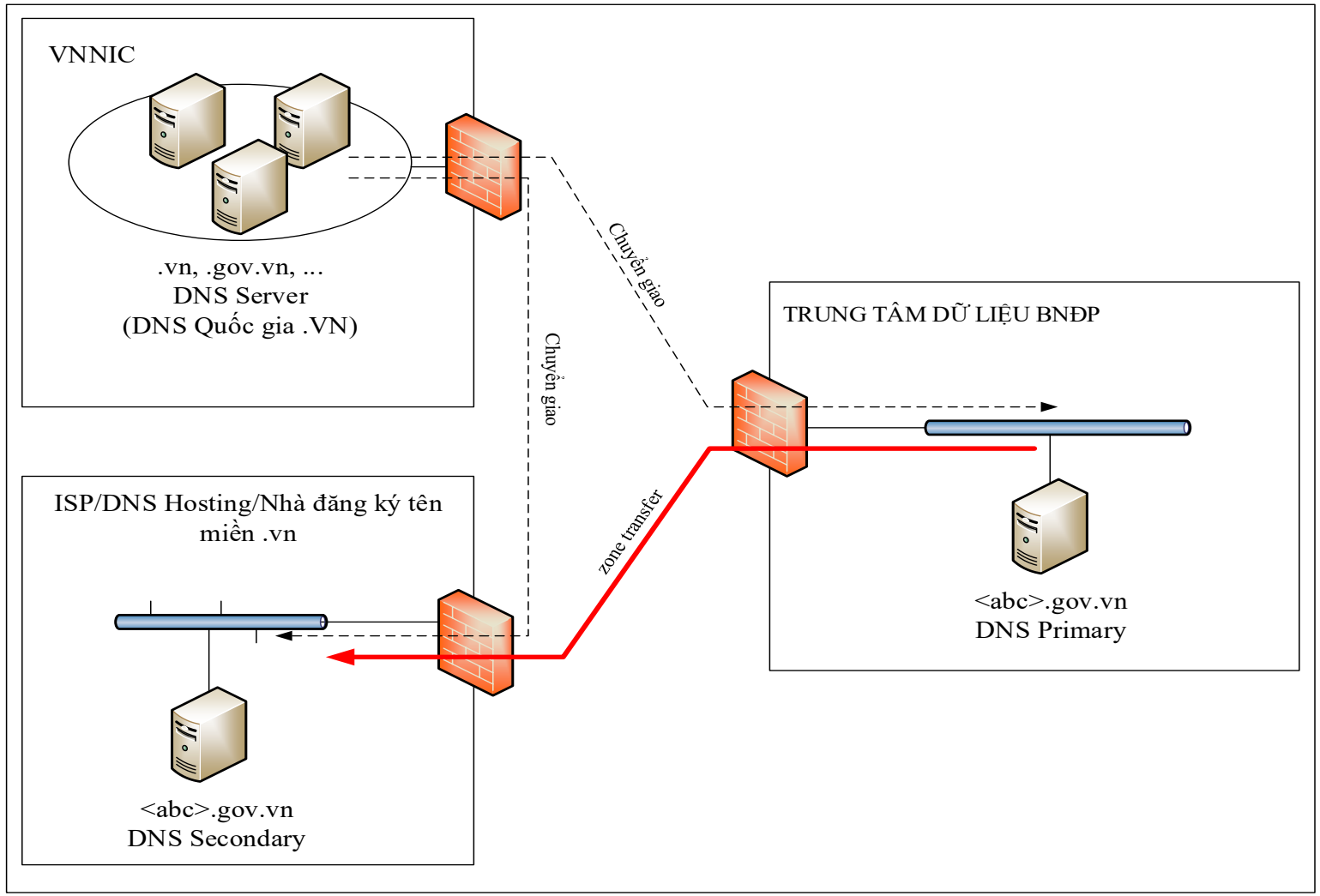
# MÔ HÌNH TIÊU CHUẨN VÀ KHUYẾN NGHỊ HỆ THỐNG DNS AUTHORITATIVE

# Nội dung

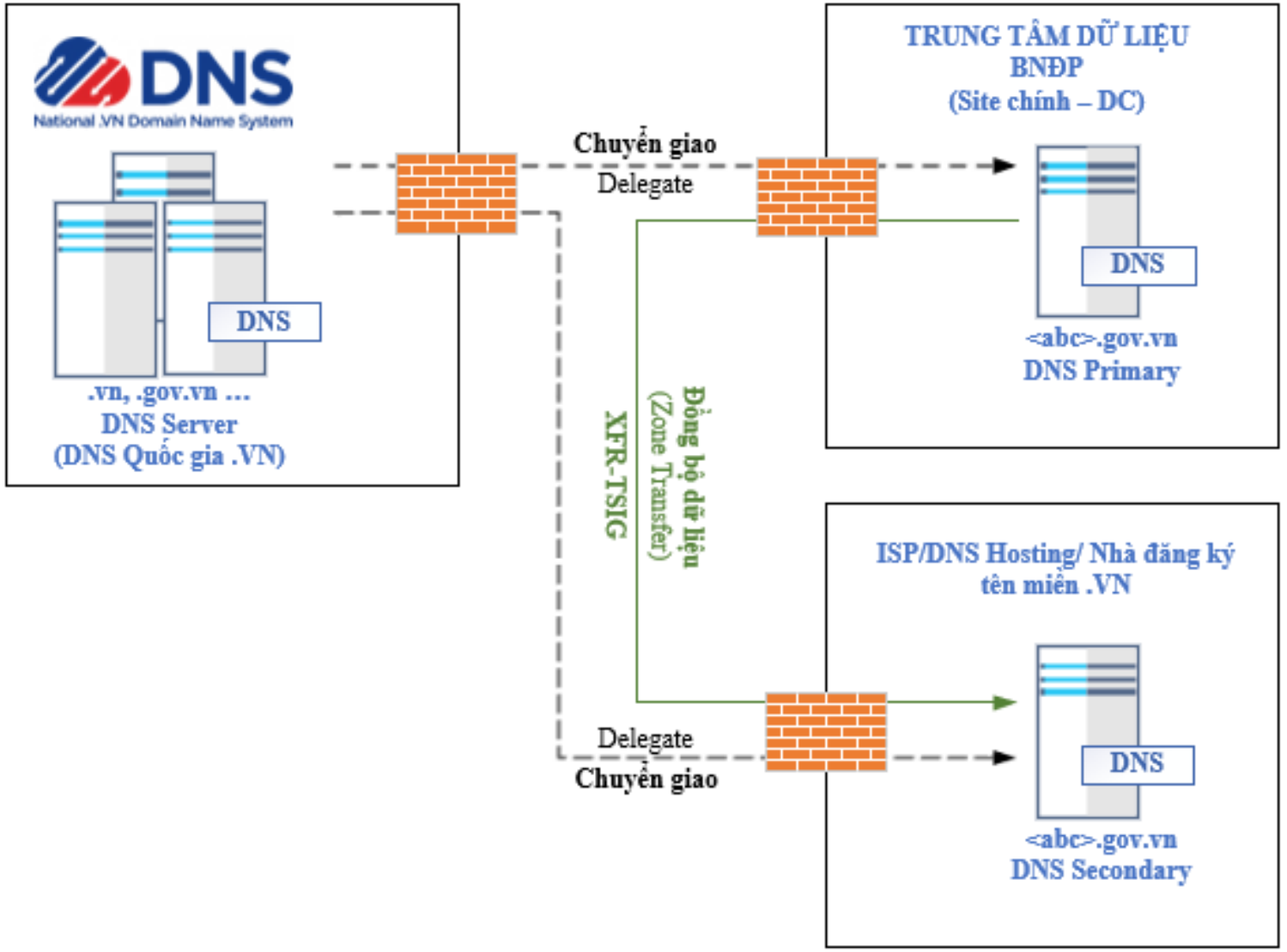
- Mô hình tiêu chuẩn
- Khuyến nghị thiết lập, cấu hình

# Mô hình tiêu chuẩn cho DNS Authoritative(1/2)

- Trích dẫn mô hình theo văn số 273/BTTTT-CBĐTW



# Mô hình tiêu chuẩn cho DNS Authoritative(2/2)



# Khuyến nghị DNS Authoritative(1/2)

- Tối thiểu 02-03 máy chủ DNS với địa chỉ IP khác nhau quản lý tên miền ở 02 mạng độc lập khác nhau.
- Triển khai mô hình Master-Slave:
  - 01 máy chủ DNS Primary (Master) quản lý dữ liệu chính, toàn bộ khai báo các bản ghi dịch vụ như <www, mail, edoc>.gov.vn được thực hiện trên máy chủ này.
  - 01-02 máy chủ DNS Secondary (Slave): được đồng bộ với máy chủ Master theo cơ chế zone transfer, sử dụng TSIG để đảm bảo an toàn (XFR + TSIG).
- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.
- Triển khai DNSSEC, đóng vai trò ký DNSSEC cho tên miền để đảm bảo an toàn tên miền.
- Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack).
- Khai báo các bản ghi AAAA cho các tên miền như <www, mail, edoc>.gov.vn để hoạt động được trên mạng IPv6.

# Khuyến nghị DNS Authoritative (2/2)

- **Khuyến nghị:**
  - Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS0 (truy vấn DNS hỗ trợ IPv6, DNSSEC).
  - Các phần mềm tham khảo:  BIND 9.x, NSD.
- **Tham khảo:**
  - Công văn số 273/BTTTT-CBĐTW ngày 31/01/2020.
  - Các tiêu chuẩn tham tham khảo: TCVN 11237-3:2015, TCVN 12044:2017; RFC1034, 1035, 1183, 1591, 3901, 4472, 4033, 4034, 4035, 4470, 4641, 5155, 6014.

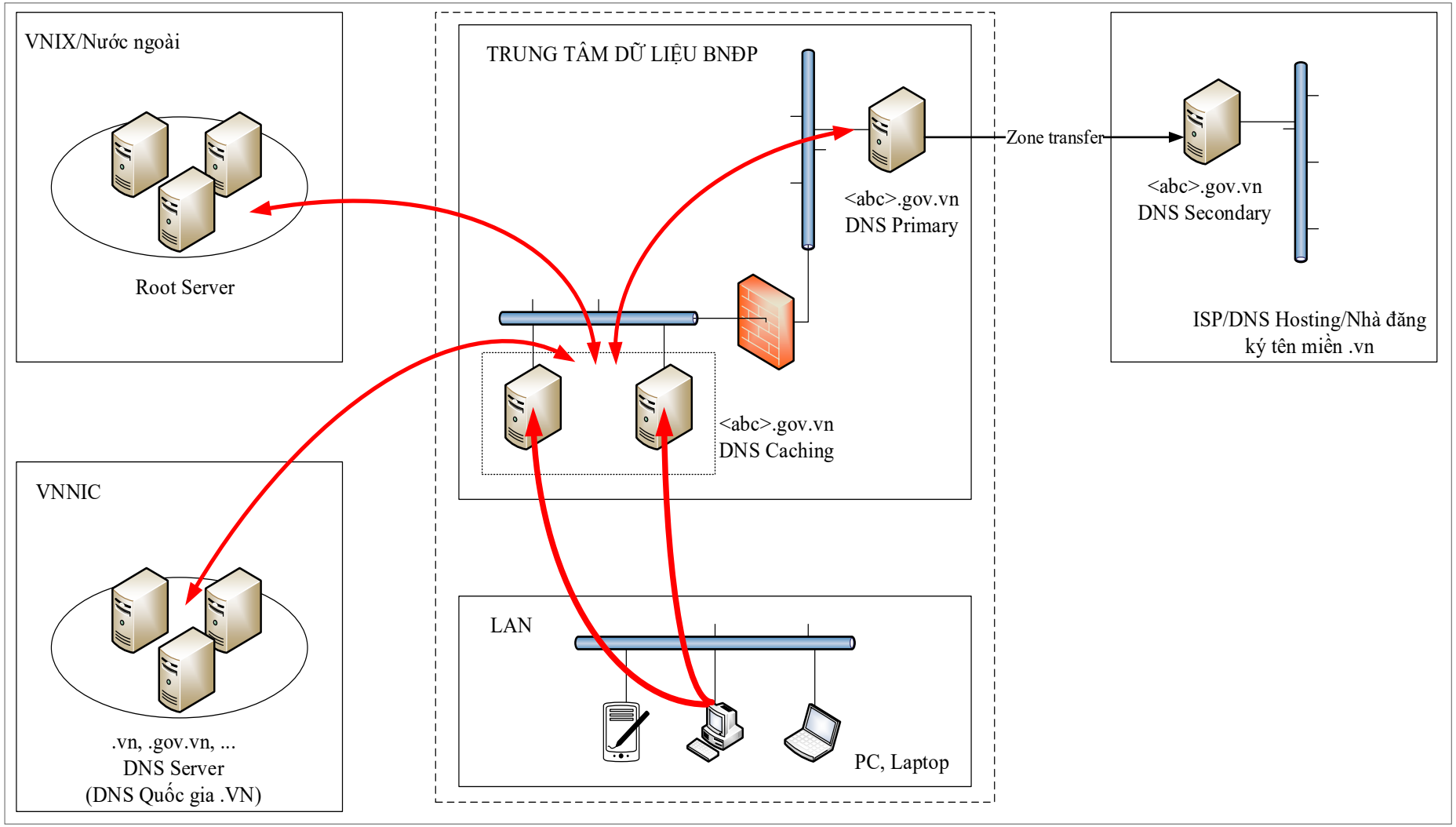
# MÔ HÌNH TIÊU CHUẨN VÀ KHUYẾN NGHỊ HỆ THỐNG DNS CACHE

# Nội dung

- Mô hình tiêu chuẩn
- Khuyến nghị thiết lập, cấu hình

# Mô hình tiêu chuẩn cho DNS Cache

- Trích dẫn mô hình theo văn số 273/BTTTT-CBĐTW



# Khuyến nghị cho DNS Cache (1/2)

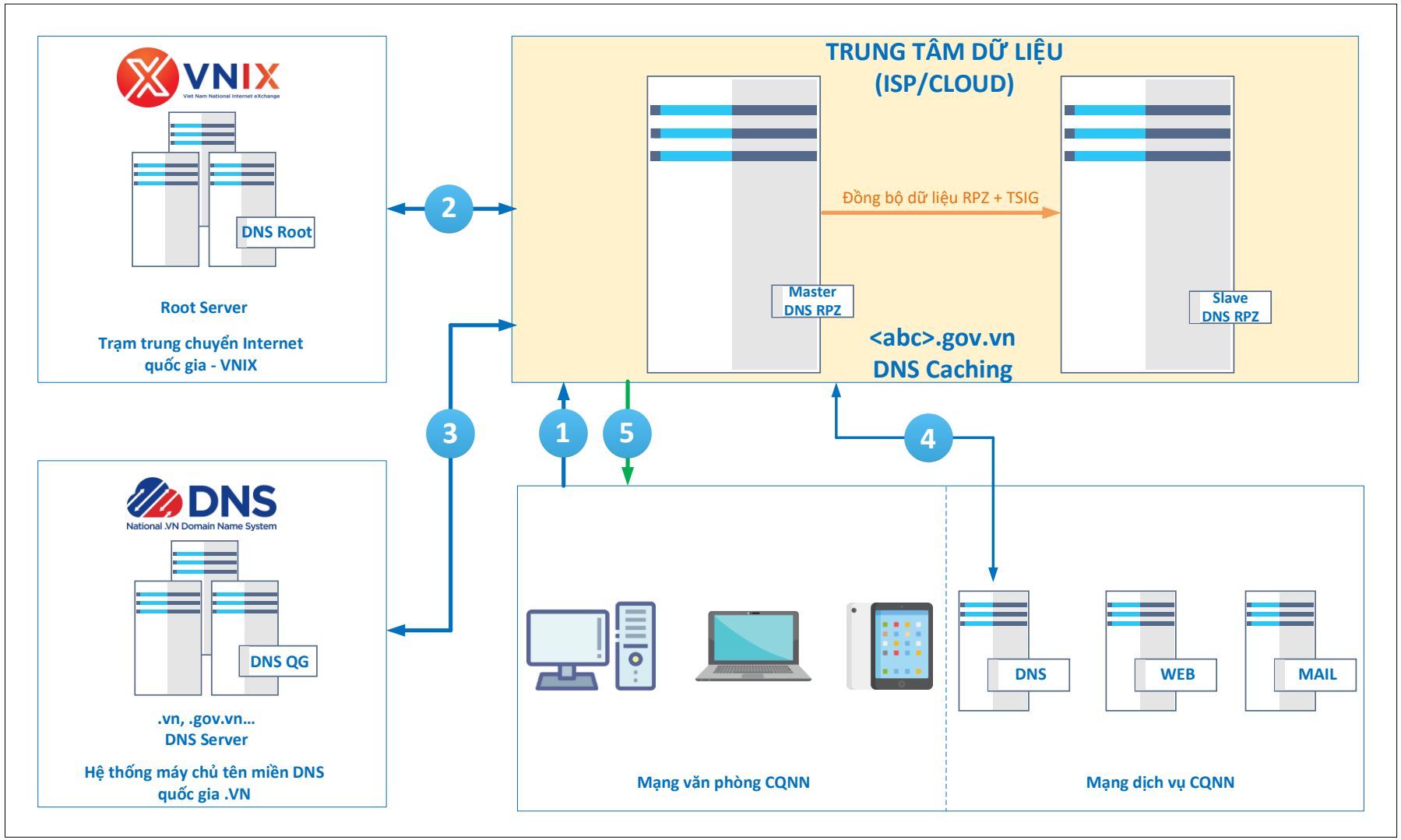
- Tối thiểu 02 máy chủ DNS Cache với địa chỉ IP khác nhau đặt tại trung tâm TTDL của BNĐP, 02 máy chủ hoạt động Active-Active, đảm bảo khả năng dự phòng nóng, khi 01 máy chủ bị lỗi hoặc hỏng hóc vẫn còn 01 máy chủ còn lại hoạt động, đảm bảo không bị gián đoạn.
- Toàn bộ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị động, …) trong mạng của đơn vị phải được cấu hình để sử dụng hệ thống DNS Cache này.
- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.
- Triển khai DNSSEC, đóng vai trò xác thực (validation) để đảm bảo an toàn tên miền.

# Khuyến nghị cho DNS Cache (2/2)

- **Khuyến nghị:**
  - Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack), hỗ trợ kết nối, truy vấn từ các máy trạm trên mạng IPv6.
  - Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS0 (truy vấn DNS hỗ trợ IPv6, DNSSEC).
  - Các phần mềm tham khảo: BIND 9.x, Unbound.
  - Triển khai DNS Internet Security: RPZ
- **Tham khảo:**
  - Công văn số 273/BTTTT-CBĐTW ngày 31/01/2020.
  - Các tiêu chuẩn tham tham khảo: TCVN 11237-3:2015, TCVN 12044:2017; RFC 1034, 1035, 1183, 1591, 3901, 4472, 4033, 4034, 4035, 4470, 4641, 5155, 6014.

# Khuyến nghị DNS Cache Internet Security

❖ Mô hình khuyến nghị



# Tài liệu tham khảo (1/3)

- **Chính sách, hướng dẫn:**
  - Luật 24/2018/QH14: Luật an ninh mạng, ngày 12/06/2018
  - Nghị định 85/2016/NĐ-CP: Về bảo đảm an toàn hệ thống thông tin theo cấp độ, ngày 01/07/2016.
  - Thông tư 12/2022/TT-BTTTT: Quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, ngày 12/08/2022.
  - Công văn 273/BTTTT-CBĐTW: Hướng dẫn mô hình tham chiếu về kết nối mạng cho bộ, ngành, địa phương, ngày 31/01/2020.

# Tài liệu tham khảo (2/3)

- **TCVN:**
  - TCVN 11930:2017 - Công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ
  - TCVN 11237-3:2015 - Giao thức cấu hình động Internet phiên bản 6 (DHCPv6)
  - TCVN 12044:2017 - Các yêu cầu bảo mật DNS (DNSSEC)
  - TCVN 7540:2005 - Hệ thống tên miền Internet - Yêu cầu kỹ thuật: Quy định yêu cầu kỹ thuật về triển khai và vận hành hệ thống DNS tại Việt Nam, gồm các quy định về cấu trúc tên miền, các loại bản ghi, thiết lập máy chủ DNS, …
  - TCVN 9160:2012 - Hệ thống tên miền Internet - Quản lý tên miền cấp quốc gia: Hướng dẫn quản lý và vận hành tên miền cấp quốc gia ".vn" tại Việt Nam; Quy định về đăng ký, gia hạn, chuyển nhượng, hủy tên miền ".vn".
  - TCVN 9161:2012 - Hệ thống tên miền Internet - Quản lý tên miền cấp nhân: Quy định về quản lý và vận hành các tên miền cấp nhân trong ".vn“, gồm các yêu cầu về đăng ký, chuyển nhượng, gia hạn, hủy tên miền cấp nhân.

# Tài liệu tham khảo (3/3)

- **RFC:**
  - RFC 1034 - Domain Names - Concepts and Facilities: Định nghĩa cơ bản về hệ thống DNS, bao gồm cấu trúc, tên miền và các loại bản ghi; Mô tả các thành phần chính như root domain, domain name space, resource records.
  - RFC 1035 - Domain Names - Implementation and Specification: Hướng dẫn chi tiết về cách triển khai và sử dụng DNS, bao gồm định dạng các gói tin, các loại bản ghi và các quy tắc; Định nghĩa các loại bản ghi DNS như A, AAAA, MX, NS, CNAME, PTR, SOA, TXT.
  - RFC 1123 - Requirements for Internet Hosts - Application and Support: Yêu cầu cơ bản đối với các máy chủ Internet, bao gồm các quy tắc liên quan đến DNS; Định nghĩa các yêu cầu về cách thức triển khai và quản lý DNS.
  - RFC 2181 - Clarifications to the DNS Specification: Cung cấp thêm các giải thích và làm rõ một số điểm trong các RFC 1034 và 1035; Hướng dẫn bổ sung về cách thức hoạt động của DNS.
  - RFC 3901 - DNS IPv6 Transport Operational Guidelines: Hướng dẫn triển khai DNS trên IPv6
  - RFC 4472 - Operational Considerations and Issues with IPv6 DNS: Các vấn đề và khuyến nghị khi triển khai DNS trên IPv6 về cấu hình máy chủ DNS, tính khả dụng, bảo mật, quản lý và vận hành.

# VI. HƯỚNG DẪN TỐI ƯU, BẢO MẬT

# VI. HƯỚNG DẪN TỐI ƯU, BẢO MẬT

# Nội dung

- Tối ưu thiết kế
- Tối ưu cấu hình
- Tối ưu dữ liệu

# Tối ưu thiết kế hệ thống DNS

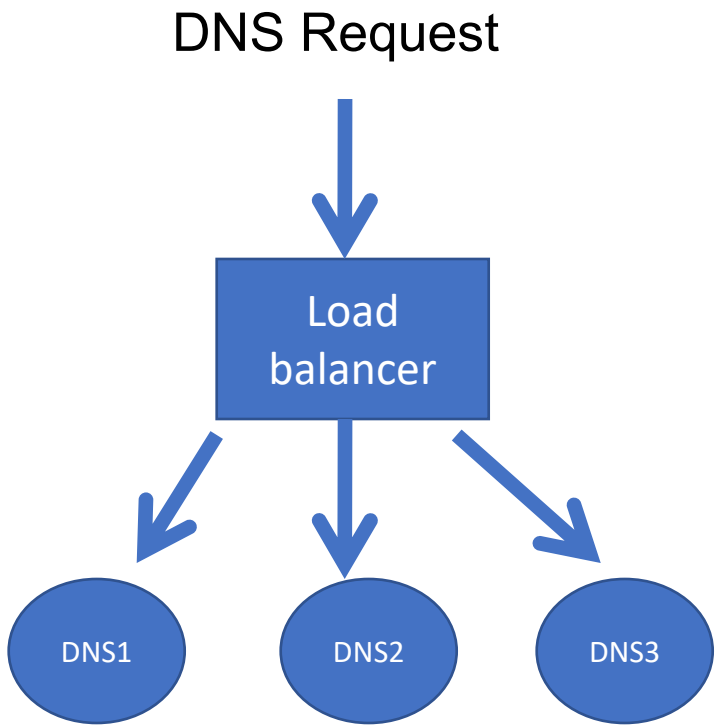
- Triển khai mô hình Master-Slave, với DNS Master không phục vụ truy vấn từ bên ngoài
- Đồng bộ dữ liệu qua AXFR hoặc IXFR
- Sử dụng DNS Slave, tối đa 13 cụm máy chủ
  - Sử dụng Cluster các máy chủ DNS
  - Sử dụng các cụm Anycast
- Triển khai tại nhiều vị trí khác nhau
  - Tăng tốc độ trả lời
  - Tăng khả năng dự phòng
- Triển khai đa dạng hóa HĐH và phần mềm

# Cluster DNS (1/2)

- Sử dụng các giải pháp cân bằng tải bằng thiết bị chuyên dùng
- Tăng cường năng lực cho cụm máy chủ DNS
- Khả năng mở rộng dễ dàng
- Phù hợp với triển khai local
- Trong suốt với người sử dụng
- Khả năng mở rộng phụ thuộc vào năng lực của thiết bị cân bằng tải
- Có khả năng phân chia tải cho các máy chủ DNS theo nhiều tham số khác nhau
- Không có khả năng chống DDOS
- Triển khai đơn giản
- Quản lý đơn giản

# Cluster DNS (2/2)

- Sử dụng thiết bị cân bằng tải.
- Phân chia các request truy vấn DNS tới các máy chủ DNS
- Hoàn toàn trong suốt với client.
- Khả năng thiết lập chính sách mở rộng linh hoạt

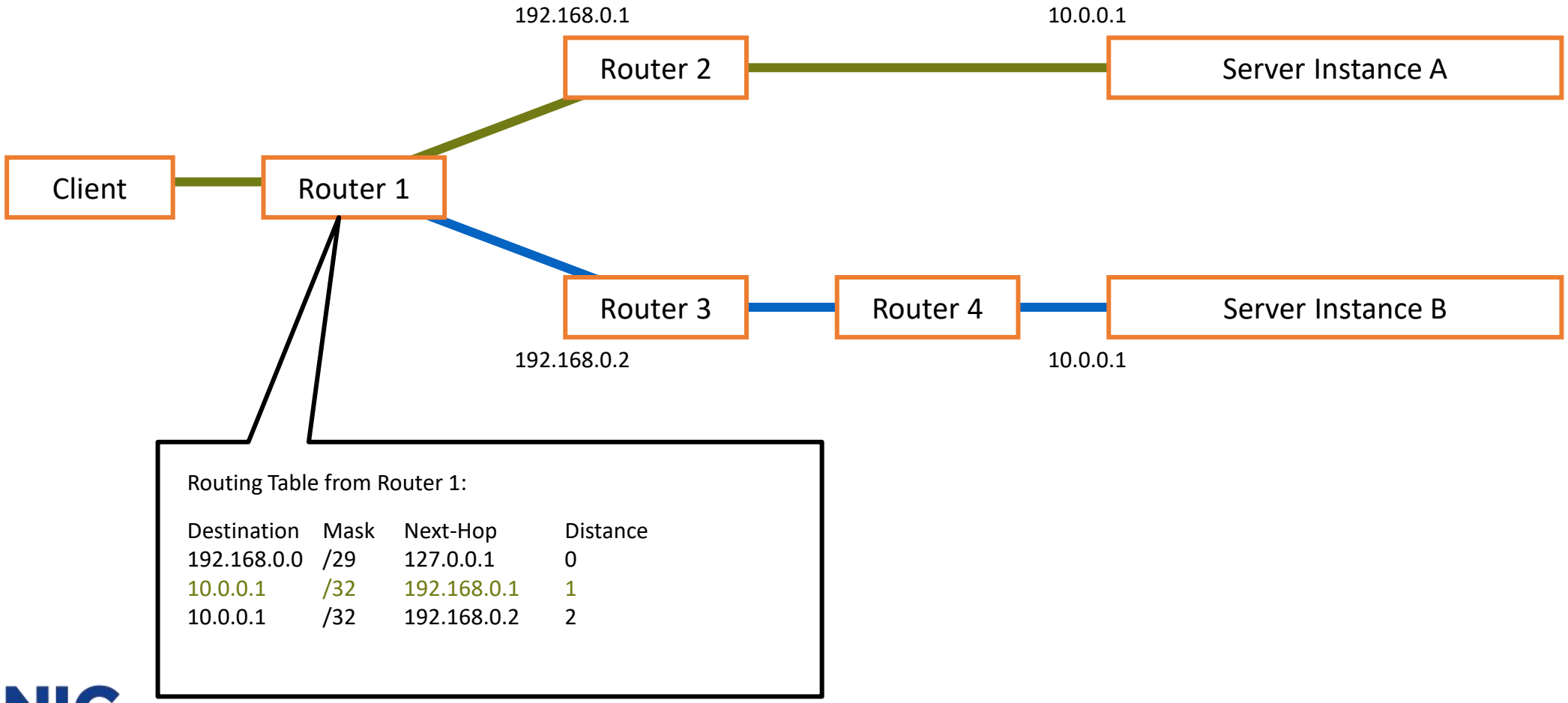


# DNS Anycast (1/2)

- Sử dụng công nghệ định tuyến địa chỉ Unicast
- Nhiều máy chủ chia sẻ 1 địa chỉ IP
- Triển khai local hoặc global
- Cho phép mở rộng “không giới hạn”
- Hoàn toàn trong suốt với người sử dụng
- Năng lực hệ thống mở rộng lên rất nhiều lần
- Áp dụng ở Root, gTLD, ccTLD lớn
- Có khả năng chống được DOS, DDOS
- Triển khai phức tạp
- Quản lý phức tạp

# DNS Anycast (2/2)

- Router sử dụng bảng định tuyến chuyển gói tin theo đường ngắn nhất.



# Tối ưu cấu hình

- Cấu hình địa chỉ dịch vụ:
  - version
  - Listen-on { 10.0.0.1; 127.0.0.1};
- Cấu hình các tham số:
  - source-query
  - source-transfer
  - notify-on
  - allow-transfer, allow-query
- Thiết lập ghi nhật ký:
  - Phân tách các loại log thành các file dễ theo dõi
  - Quản lý vòng đời của file.
- Thiết lập thống kê (Statistic): thu thập và lưu trữ các số liệu thống kê liên quan đến một vùng.

# Tối ưu sử dụng DNS Cache

- Các thông tin về câu trả lời nhận được từ các máy chủ tên miền sẽ được lưu lại trong một khoảng thời gian, thời gian này theo giá trị TTL của từng bản ghi tài nguyên tương ứng, giúp cho hoạt động truy vấn tên miền nhanh chóng, giảm tải cho các máy chủ.
    - Nếu giá trị TTL của bản ghi tài nguyên nhỏ, dữ liệu sẽ được cập nhật thường xuyên, sẽ được đảm bảo tính chính xác, tuy nhiên các máy chủ tên miền và DNS Cache sẽ phải chịu tải nhiều hơn.
    - Nếu giá trị TTL của bản ghi tài nguyên lớn, dữ liệu không thường xuyên được cập nhật có thể không đảm bảo tính chính xác của bản ghi.
- RFC 1912: Common DNS Operational and Configuration Errors

# Tối ưu cấu hình- DNS Cache

- Thiết lập thời gian negative-cache tối đa
  - max-ncache-ttl
  - Mặc định: 3 hours, max 7 days
  - Nếu thiết lập > 7 days, BIND đặt lại thành 7 days
- Thiết lập thời gian cache tối đa:
  - max-cache-ttl
  - Mặc định: 1 week
- Thiết lập thời gian xóa bản ghi có TTL đã expire
  - cleaning-interval
  - Mặc định 60 mins

# Tối ưu cấu hình - Tham số trong bản ghi SOA

- Tối ưu:
  - Serial number
  - Thiết lập thời gian refresh
  - Thiết lập thời gian update retry
  - Thiết lập thời gian expire
  - Thiết lập Negative TTL
- RFC 1912: Common DNS Operational and Configuration Errors

# Tối ưu cấu hình - Đồng bộ dữ liệu Zone Transfer

- Đặt Max/Min tần suất zone transfer
- Khai báo: min-refresh-time, max-refresh-time, min-retry-time, max-retry-time:
- Sử dụng ở máy chủ Slave, ưu tiên hơn giá trị thiết lập ở bản ghi SOA của zone.
- Thiết lập các mức global, zone, view:

```
options {
    max-refresh-time 86400;     // refresh should never be more than a day
    min-refresh-time 1800;     // or less than 30 minutes
};
```

# Tối ưu dữ liệu - Sử dụng bản ghi CNAME

```
www   IN  A   10.0.0.1
web   IN  A   10.0.0.1
server  IN  A  10.0.0.1
```

```
www  IN   A   10.0.0.1
web  IN   CNAME   www
server  IN   CNAME   www
```

# Tối ưu dữ liệu - Sử dụng bản ghi TXT

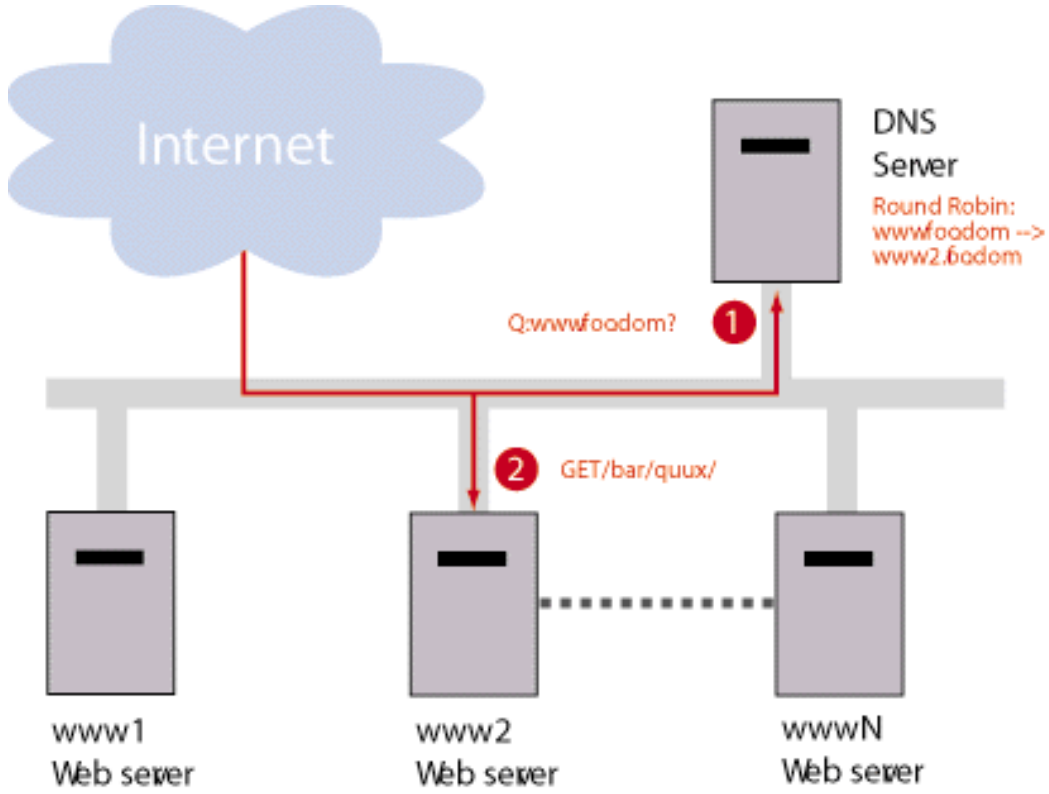
- Cung cấp thêm thông tin về Zone, Email Authentication, SSL, …
- Ví dụ:

*mail IN A 203.119.8.101*

*mail IN TXT “VNNIC Mail server No1 in HN*

# Cân bằng tải dịch vụ Round-Robin DNS

- **Ưu điểm:**
  - Khái niệm đơn giản
  - Không yêu cầu thêm phần cứng.
- **Nhược điểm:**
  - DNS không nhận biết được trạng thái của web servers
  - Tất cả các server được xem như có năng lực như nhau với tất cả các dịch vụ.



# Tối ưu dữ liệu – Sử dụng cân bằng tải dịch vụ

- RFC1794 - DNS Support for Load Balancing
- BIND hỗ trợ thiết lập hoạt động cân bằn tải dịch vụ round-robin và trật tự điều khiển trật tự của các RR giống nhau thông qua tham số rrset-order, có giá trị mặc định là random-cyclic (khi trả lời các truy vấn, BIND sẽ thay đổi thứ tự các địa chỉ IP theo một cách ngẫu nhiên, nhưng đảm bảo rằng mỗi địa chỉ IP sẽ được trả về đúng một lần trong một chu kỳ)
- **Flie cấu hình:**

```
// named.conf fragment
options {
// other options
rrset-order {order cyclic;};
};
```

- **File dữ liệu:**

```
ftp   IN  A   192.168.0.4
ftp   IN  A   192.168.0.5
ftp   IN  A   192.168.0.6
www   IN  A   192.168.0.7
www   IN  A   192.168.0.8
```

# Tối ưu dữ liệu – Sử dụng cân bằng tải Mail

- Một số phần mềm Mail có cơ chế xử lý các bản ghi có cùng mức độ ưu tiên
- **Cách 1:**

```
; zone file fragment
IN   MX    10    mail.example.com.
IN   MX    10    mail1.example.com.
IN   MX    10    mail2.example.com.

mail    IN    A    192.168.0.4
mail1   IN    A    192.168.0.5
mail2   IN    A    192.168.0.6
```

- **Cách 2:**

```
; zone file fragment
        IN   MX   10  mail.example.com.
mail    IN   A    192.168.0.4
        IN   A    192.168.0.5
        IN   A    192.168.0.6
```

# BẢO MẬT DỊCH VỤ, HỆ THỐNG DNS

# Nội dung

- Tổng quan đảm bảo an toàn hệ thống
- Thiết kế mô hình hệ thống đảm bảo an toàn
- Thiết lập cấu hình đảm bảo an toàn
  - Máy chủ DNS Authentative
  - Máy chủ DNS Cache
- Triển khai giải pháp đảm bảo an toàn

# Tổng quan đảm bảo an toàn hệ thống

- **Đảm bảo an toàn vật lý:**
  - Kiểm soát truy cập ở mức vật lý
- **Đảm bảo an toàn mạng**
  - Thiết lập tường lửa giới hạn truy cập dịch vụ
  - Đảm bảo an toàn truy cập mạng (từ xa, trong mạng)
- **Đảm bảo an toàn máy chủ**
  - Giới hạn, kiểm soát, xác thực truy cập HĐH
  - Cập nhật, vá lỗi HĐH
- **Đảm bảo an toàn dịch vụ**
  - Mô hình: dự phòng, cân bằng tải
  - Công nghệ: bảo mật, cân bằng tải
  - Chạy dịch vụ sử dụng Chroot
  - Thiết lập các tham số hạn chế
  - Ghi nhật ký
  - Cập nhật, vá lỗi HĐH
- **Đảm bảo an toàn dữ liệu**
  - Thiết lập đảm bảo trong cập nhật, đồng bộ dữ liệu
  - Kiểm soát truy cập các file cấu hình, file dữ liệu
  - Sao lưu dự phòng dữ liệu

# Tối ưu đảm bảo an toàn và năng lực

- Thiết kế mô hình hệ thống
- Thiết lập cấu hình
- Thiết lập thông tin bản ghi tài nguyên
- Triển khai công nghệ

# Thiết kế mô hình hệ thống

| Thiết kế | Hệ thống máy chủ DNS Authoritative | Hệ thống máy chủ DNS Cache |
|---|---|---|
| Mô hình Master-Slave, DNS Stealth | ✓ | |
| Multimaster | ✓ | |
| Mô hình Split và View | ✓ | |
| Triển khai tối thiểu 02 máy chủ tiếp nhận truy vấn đặt sử dụng 02 địa chi IP thuộc 02 dải mạng ở vị trí địa lý | ✓ | ✓ |
| Triển khai đa dạng hóa HĐH và phần mềm dịch vụ | ✓ | ✓ |
| Cân bằng tải Load Balace: F5, Anycast | ✓ | ✓ |

# Thiết lập máy chủ DNS Authoritative

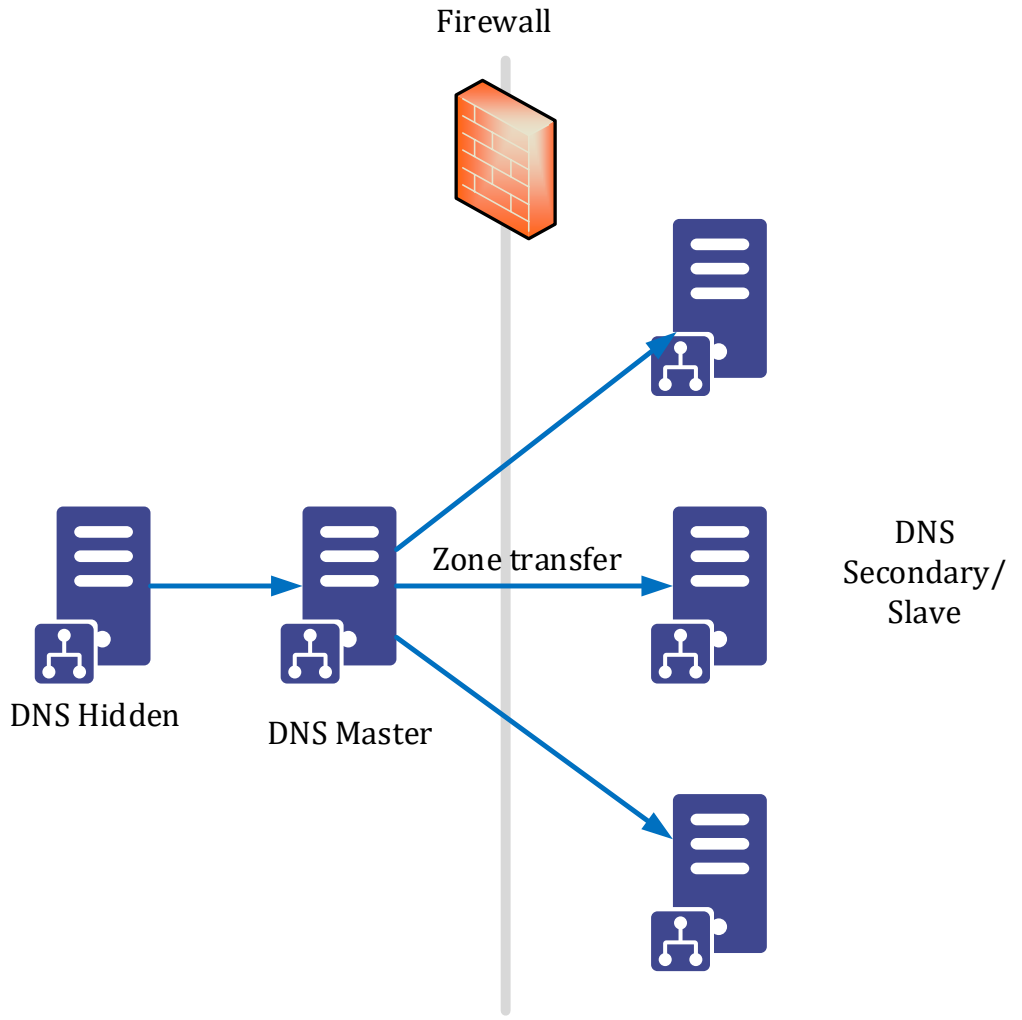
| Nội dung | Hướng dẫn |
|---|---|
| Chạy dịch vụ ở chế độ chroot, phân quyền file cấu hình, dịch vụ | |
| Thiết lập chế độ non-recursive | recursion no; |
| Thiết lập ẩn phiên bản phần mềm | version |
| Thiết lập thông tin giới hạn đảm bảo an toàn cho hoạt động truy vấn | ACL<br>listen-on, listen-on-v6, allow-query, source-query |
| Thiết lập thông tin giới hạn đảm bảo an toàn cho hoạt động cập nhật, đồng bộ dữ liệu | - Giới hạn địa chỉ IP cập nhật dữ liệu: allow-query<br>- Chỉ cho phép giới hạn địa chỉ IP trong quá trình đồng bộ, thông báo: allow-transfer, source-transfer, allow-notify, also-notify, …<br>- Tối ưu các giá trị thời gian liên quan đồng bộ dữ liệu: thiết lập trong bản ghi SOA (RFC 1912), min-refresh-time, max-refresh-time, minretry-time, max-retry-time, …<br>- Thiết lập chế độ đồng bộ: AXFR (toàn bộ) hoặc IXFR (nội dung thay đổi)<br>- Sử dụng TSIG cho quá trình cập nhật, đồng bộ dữ liệu an toàn |
| Thiết lập ghi nhật ký | - Thiết lập ghi các loại nhật ký khác nhau (truy vấn, dnssec, debug, zone transfer, …)<br>- Thiết lập quản lý vòng đời của file nhật ký |
| Thiết lập thống kê truy vấn | zone-statistics |
| Thiết lập giới hạn truy vấn tiếp nhận | Response Rate Limit (RRL), Blackhole |

# Thiết lập máy chủ DNS Cache

| Nội dung | Hướng dẫn |
|---|---|
| Chạy dịch vụ ở chế độ chroot, phân quyền file cấu hình, dịch vụ | |
| Thiết lập chế độ recursive | recursion yes; |
| Thiết lập ẩn phiên bản phần mềm | version |
| Thiết lập thông tin giới hạn đảm bảo an toàn cho hoạt động truy vấn | listen-on, listen-on-v6<br>allow-query, source-query |
| Thiết lập các thông số thời gian lưu Cache | - Thiết lập thời gian negative-cache tối đa:<br>max-ncache-ttl<br>Mặc định: 3 giờ, max 7 ngày<br>Nếu thiết lập > 7 ngày, BIND đặt lại thành 7 ngày.<br>- Thiết lập thời gian cache tối đa<br>max-cache-ttl<br>Mặc định: 7 ngày.<br>- Thiết lập thời gian xóa bản ghi có TTL đã expire<br>cleaning-interval<br>Mặc định 60 phút. |
| Thiết lập RPZ | |

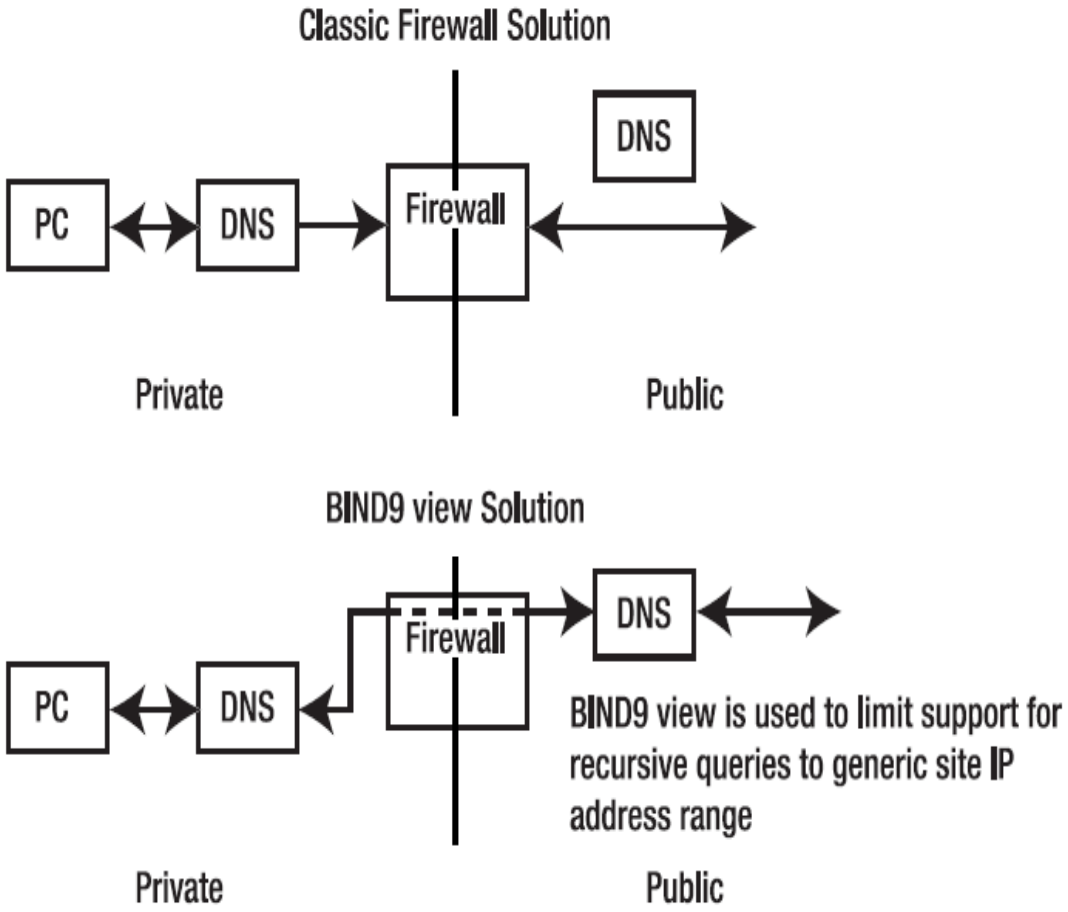
# Triển khai mô hình Master - Slave

- 01 Master của cụm DNS với nhiều Slave:
  - Máy chủ Master chứa dữ liệu tên miền gốc đặt trong phân mạng bảo mật, DNS Master (Hidden Master) không phục vụ truy vấn từ bên ngoài.
  - Máy chủ Slave nhận đồng bộ dữ liệu từ các máy chủ Master đặt ở các phân mạng Public để tiếp nhận dịch vụ từ người dùng hoặc đặt ở phân mạng bảo mật sử dụng cho mục đích Backup không tiếp nhận truy vấn từ người dùng.
- Đồng bộ dữ liệu qua AXFR hoặc IXFR



# Triển khai mô hình Split

- Địa chỉ nguồn khác nhau → có câu trả lời khác nhau:
  - Thực hiện bằng cách 02 DNS đặt 02 phân mạng khác nhau của Firewall
  - Hoặc sử dụng cơ chế View của BIND (chỉ cần 01 DNS)



# Cấu hình View

```
// internal hosts view
view "goodguys" {
match-clients { 192.168.254.0/24; };
recursion yes;
zone "." {      // required zone for recursive queries
type hint;
file "root.servers";
};
zone "example.com" {
      type master;
      // private zone files including local hosts
      file "view/master.example.com.internal";
      allow-update {none;};
      };
// reverse map for local address at example.com
// uses 192.168.254.0 for illustration
zone "254.168.192.IN-ADDR.ARPA" in{
      type master;
      file "view/192.168.254.rev.internal";
      allow-update {none;};
};
}; // end view
```

```
// external hosts view
view "badguys" {
match-clients {"any"; }; // all other hosts
// recursion not supported
recursion no;
zone "example.com" {
      type master;
      // only public hosts
      file "view/master.example.com.external";
      allow-update {none;};
};
// reverse map for local address at example.com
// uses 192.168.254.0 for illustration
zone "254.168.192.IN-ADDR.ARPA" in{
      type master;
      file "view/192.168.254.rev.external";
      allow-update {none;};
};
}; // end view
```

VNNIC Internet for all

# TSIG - Transaction SIGnature

- TSIG (Transaction SIGnature) được sử dụng để bảo vệ: Dynamic Update, Zone Transfer.
- Để sử dụng TSIG cả phía nhận và phía gửi phải được cấu hình sử dụng một khoá chung (sharedkey).
- Gói tin gửi đi sẽ được hashing bằng khoá chung này. Phía nhận và phía gửi sẽ sử dụng khoá chung để xác thực dữ liệu đảm bảo dữ liệu không bị thay đổi.

# Các tham số hạn chế

- BIND cung cấp các tham số allow
  - allow-query: Xác định clients được phép truy vấn thông tin của 1 zone. Mặc định cho phép tất cả truy vấn.
  - allow-transfer: Xác định máy chủ Slave được phép truy vấn thông tin của zone. Mặc định cho phép tất cả các yêu cầu truy vấn.
  - allow-update: Xác định máy tính được phép cập nhật động (dynamic update) thông tin của zone. Mặc định cho cấm tất cả các yêu cầu cập nhật động.
  - allow-recursion: Xác định clients được phép truy vấn đệ quy. Mặc định cho phép tất cả.
- Thiết lập global hoặc zone

# Sử dụng ACL

- Định nghĩa một danh sách IP
- Để thực hiện cho phép/không cho phép một hoạt động nào đó trên DNS
- Cấu trúc:
  - acl acl-name { address_match_list } ;
  - Có thể sử dụng dấu !  -> loại trừ (exclusive)
  - address_match_list: any, none, localhost, localnet
- Có thể khai báo nhiều ACL với acl-name khác nhau.
- Ví dụ:

*acl "my-networks" {195.47.37.0/24; 195.47.31.0/24; }; // definition of the IP addresses group*

# Blackhole

- Định nghĩa 1 danh sách IP mà server không tương tác hoặc trả lời truy vấn.
- Mặc định: chấp nhận tất cả.
- Sử dụng ở chế độ global.
- Cấu trúc:
  - blackhole { address_match_list };
  - blackhole { none; };  mặc định none

# Cấu hình ACL

- **Global**

```
acl "my-networks" {195.47.37.0/24; 195.47.31.0/24; }; // definition of the IP addresses group

options {
        directory "/var/named";
        allow-query {"my-networks";};
};

zone "example.vn" {
      type master;
      file "example.vn.db";
      notify yes;
};
```

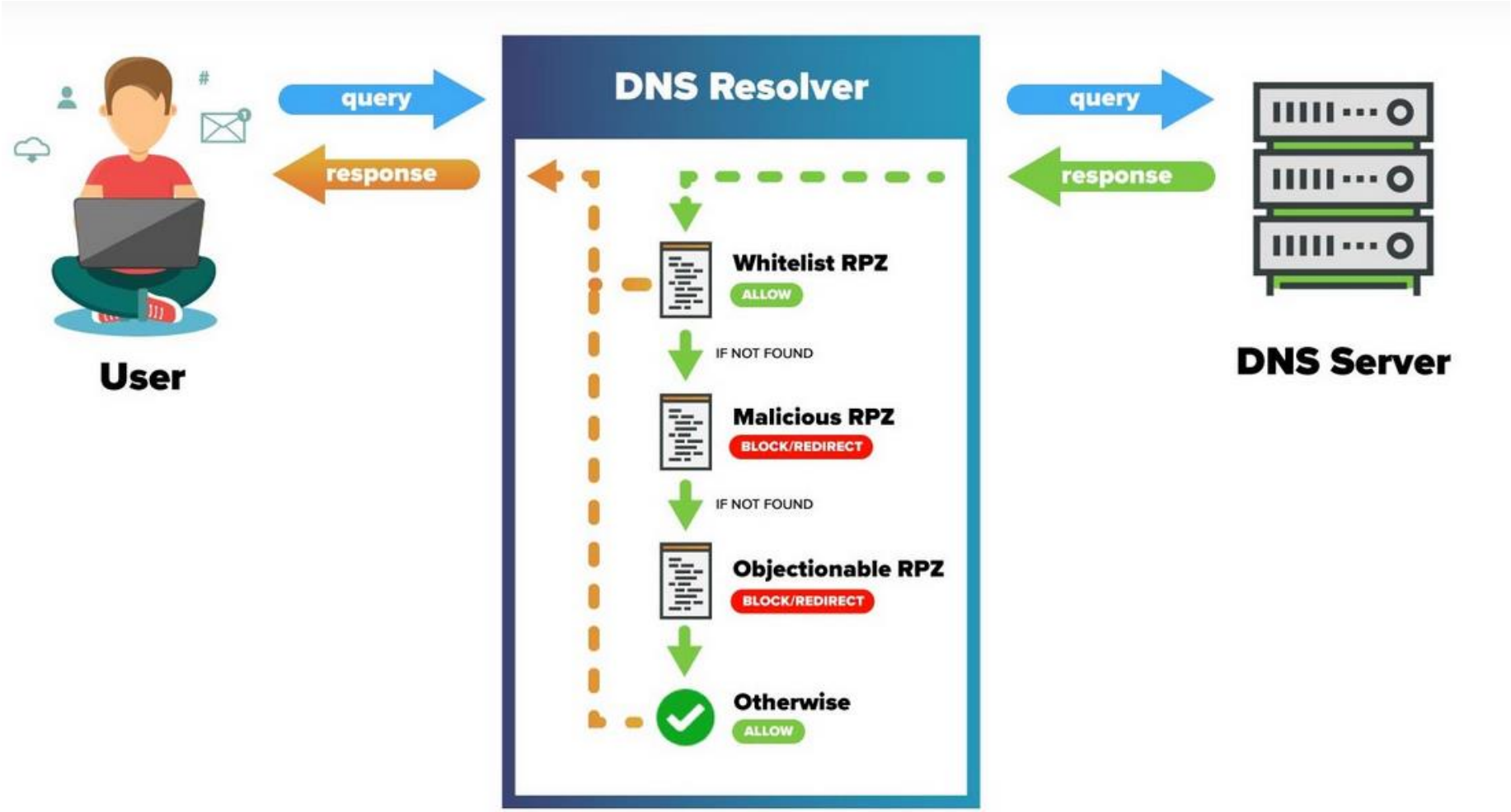
- **Zone**

```
acl "my-networks" {195.47.37.0/24; 195.47.31.0/24; }; // definition of the IP addresses group

options {
        directory "/var/named";
};

zone "example.vn" {
    type master;
    file "example.vn.db";
    notify yes;
        allow-query {"my-networks";};
};
```

# Khái quát RPZ

- RPZ trên DNS Cache hoạt động như một Firewall mềm, dựa trên hoạt động của DNS để đảm bảo an toàn cho người dùng, dịch vụ và hệ thống.
- RPZ (Response Policy Zone):
  - Cho phép DNS Cache kiểm soát việc phản hồi truy vấn trên DNS Cache.
  - Dữ liệu được hỗ trợ như zone DNS và hoạt động đồng bộ.
  - Chặn phản hồi truy vấn, chặn kết nối đến các địa chỉ C&C, máy chủ chứa mã độc, nguồn tên miền độc hại.

# Thiết lập RPZ



# Chức năng RPZ

- Ngăn chặn kết nối của người dùng đến các địa chỉ C&C, máy chủ chứa mã độc, nguồn tên miền độc hại:
  - Chặn Phishing (lừa đảo)
  - Chặn Malware (phần mềm độc hại)
  - Chặn Ransomeware (phần mềm độc hại)
  - Chặn Botnet
  - Xác định máy chủ nhiễm mã độc hoặc bị Botnet.

# Cơ chế hoạt động của RPZ (1/2)

- RPZ đặt các rule (quy luật) bao gồm các bộ lọc để phần hồi truy vấn, để từ kết quả được lọc đó thực hiện theo một danh sách có sẵn.
  - Danh sách các đối tượng sử dụng đưa vào bộ lọc bao gồm:
  - Domain (tên miền)
  - IP xuất hiện trong nội dung phản hồi
  - Tên hoặc IP của máy chủ DNS Authoritative nhận được trong quá trình phân giải việc chuyển giao.
  - Địa chỉ của người dùng

# Cơ chế hoạt động của RPZ (2/2)

- Dựa trên các quy luật đã thiết lập chính sách để thực hiện một số hành động:
  - Phản hồi NXDOMAIN (tên miền không tồn tại)
  - Phản hồi NODATA (tên miền tồn tại, nhưng không có bản ghi phản hồi).
  - Chuyển hướng người dùng sang truy cập một domain khác (CNAME tên miền gốc được truy vấn)
  - Thay thế nội dung trả lời bằng nội dung cụ thể được thiết lập.
  - Gửi yêu cầu thực hiện truy vấn lại sử dụng TCP.
  - Phản hồi thông thường.
  - Không phản hồi.

# Thiết lập RPZ (1/3)

- RPZ được hỗ trợ trên một số phần mềm DNS phổ biến cho DNS Cache như:
  - BIND 9.9 (hoặc cao hơn)
  - Power DNS
- Một số DNS Cache đã thiết lập RPZ để hoạt động như:
  - Infloxblox
  - Efficient IP
  - BlueCat

# Thiết lập RPZ (2/3)

❖ **Đưa zone vào áp dụng các rule của RPZ**

```
response-policy {
        zone "rpz-local";
        zone "tor-exit-nodes.local";
        zone "drop.rpz.spamhaus.org";
};
```

❖ **Thiết lập zone**

```
zone "drop.rpz.spamhaus.org" {
        type slave;
        file "dbx.drop.rpz.spamhaus.org";
        masters {
                X.X.X.X;
                X.X.X.X; };;
        allow-transfer { none; };;
        allow-query { localhost; };;
};
```

❖ **Cấu hình log**

```
channel rpzlog {
        file "rpz.log" versions unlimited size 1000m;
print-  time yes;
        print-category yes;
        print-severity yes;
        severity info;
};
        category rpz { rpzlog; };;
```

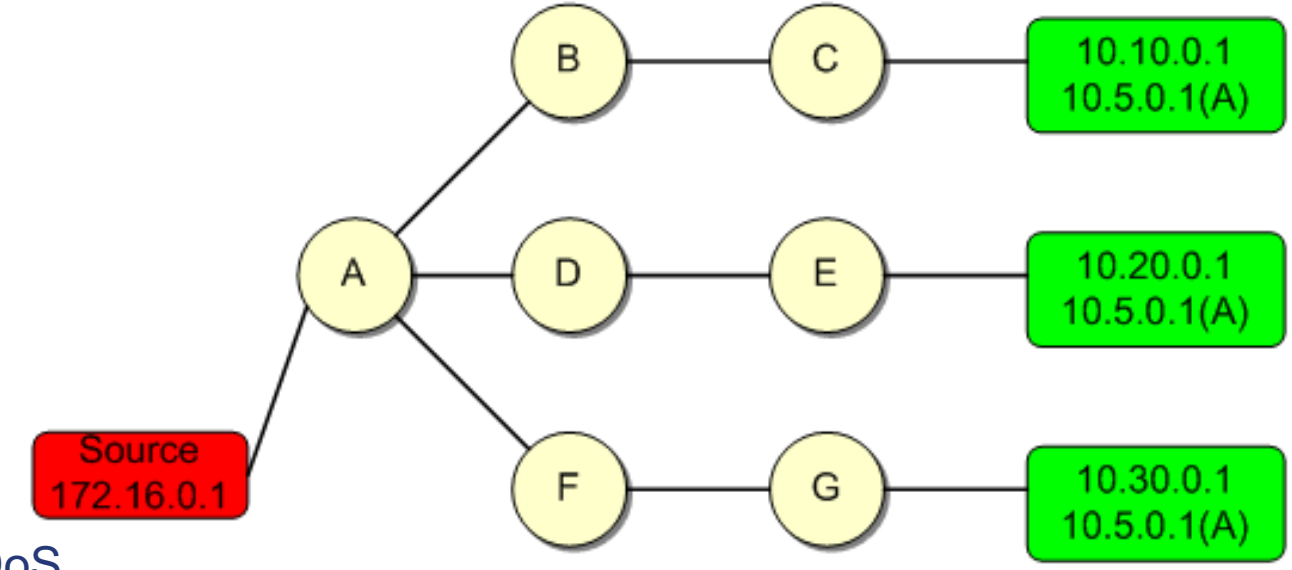
# DNSSEC

- DNSSEC là công nghệ an toàn mở rộng của hệ thống DNS
- DNSSEC không làm thay đổi cấu trúc và nền tang giao thức DNS, tiến trình truyền dữ liệu DNS và quá trình chuyển giao từ các DNS cấp cao xuống các DNS cấp thấp hơn (cùng tồn tại với hạ tầng hiện tại).
- Thay đổi mô hình DNS từ mô hình mở (open) sang mô hình tin cậy (trusting) và xác thực (verifiable).
- Người dùng Internet sử dụng DNSSEC được kiểm tra xác thực, toàn vẹn dữ liệu, đảm bảo truy cập an toàn.

# Anycast

- **Anycast** là một khái niệm thông tin truyền bất kỳ hướng nào, cụ thể là một gói tin được gởi tới một địa chỉ đơn bất kì hướng nào sẽ được chuyển tới một node (hay giao diện) gần nhất (gần nhất là khoảng cách gần nhất xác định qua giao thức định tuyến sử dụng) trong tập hợp node mang địa chỉ anycast đó.

- Ứng dụng Anycast trong hoạt động DNS là các máy chủ DNS được cấu hình cùng 01 địa chỉ IP tiếp nhận truy vấn từ người dùng.
  - Tận dụng cơ hở hạ tầng sẵn có.
  - Cân bằng tải
  - Tăng độ linh động
  - Cải tiến về trễ
  - Cơ chế phân tán, giảm nguy cơ DoS



# VII. DNS IPV6

# Nội dung

- Ánh xạ tên miền và địa chỉ IPv6
  - Phân giải tên miền thuận trong IPv6
  - Phân giải tên miền ngược trong IPv6
  - Các bản ghi tên miền
- Quá trình truy vấn, phân giải
  - Giao thức truyền tải
  - EDNS0
- Cấu hình IPv6 và khai báo bản ghi AAAA, PTR
- Phần mềm hỗ trợ
- Khuyến nghị cho DNS hoạt động IPv6
- Hướng dẫn triển khai DNS hoạt động IPv6
- Chuyển đổi Website IPv6

# Ánh xạ tên miền và địa chỉ IPv6

- Ánh xạ tên miền sang địa chỉ IPv4 thông qua bản ghi A, tuy nhiên bản ghi A không được xây dựng để hỗ trợ địa chỉ IPv6 với 128 bits địa chỉ.
- Hệ thống DNS hỗ trợ IPv6 từ năm 1995 thông qua RFC 1886, 3596, các RFC này đề cập đến một số vấn đề cơ bản như sau:
  - Ánh xạ tên miền sang địa chỉ IPv6 thông qua bản ghi AAAA.
  - Ánh xạ địa chỉ IPv6 sang tên miền sử dụng miền ip6.arpa.
  - Ánh xạ địa chỉ IPv6 sang tên miền sử dụng bản ghi PTR.

# Phân giải tên miền thuận trong IPv6

- Để ánh xạ một tên miền sang địa chỉ IPv6, hệ thống tên miền sử dụng kiểu bản ghi mới, gọi là bản ghi AAAA (tương đương bản ghi kiểu A trong địa chỉ IPv4). Bản ghi AAAA có dạng thức như sau:

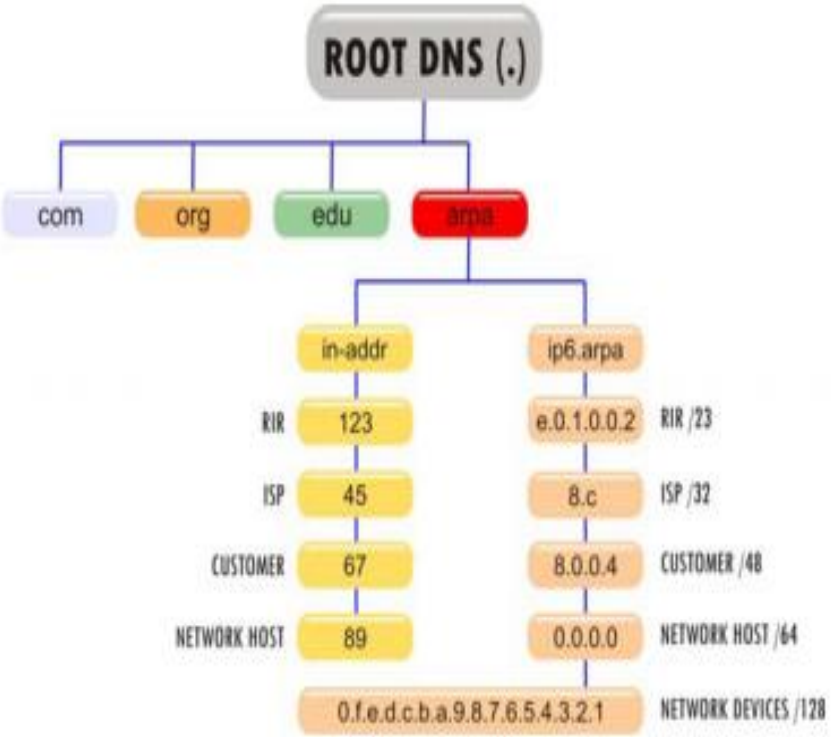
www.abc.test AAAA 3FFE:B00:C18:1::2

# Phân giải tên miền ngược trong IPv6 (1/2)

- Để ánh xạ địa chỉ IPv6 tới tên miền, hệ thống DNS cũng sử dụng kiểu bản ghi PTR, việc khai báo tên miền ngược cho tên miền khai báo ở trên như sau:

2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.0.

0.b.0.e.f.f.3.**ip6.arpa PTR** www.abc.test



# Phân giải tên miền ngược trong IPv6 (2/2)

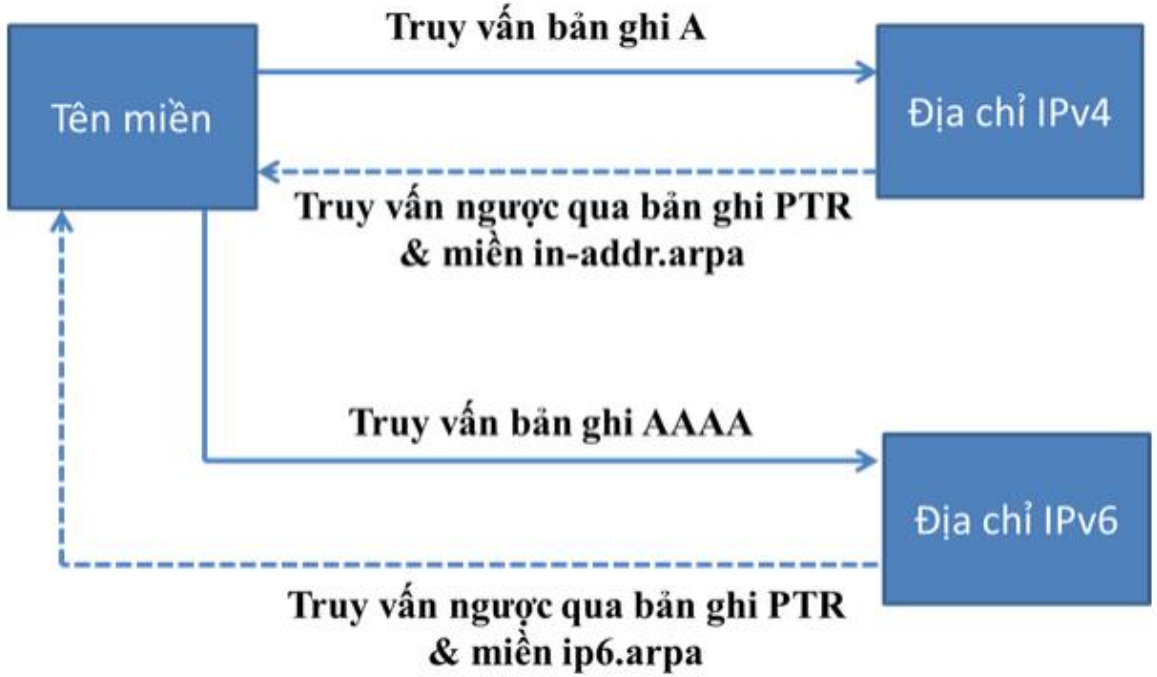
- Địa chỉ IPv4 sử dụng miền ".in-addr.arpa" cho tên miền ngược. Địa chỉ IPv4 sử dụng miền ".in-addr.arpa" cho tên miền ngược. Tên miền ngược cho địa chỉ IPv4 được chuyển giao dạng classful (/8, /16 và /24)

- Ban đầu, RFC 1886 sử dụng miền ".ip6.int" để khai báo tên miền ngược, sau này miền ".ip6.int" được hủy bỏ. Tên miền ngược IPv6 được khai báo và chuyển giao trong không miền ".ip6.arpa" của hệ thống tên miền toàn cầu.

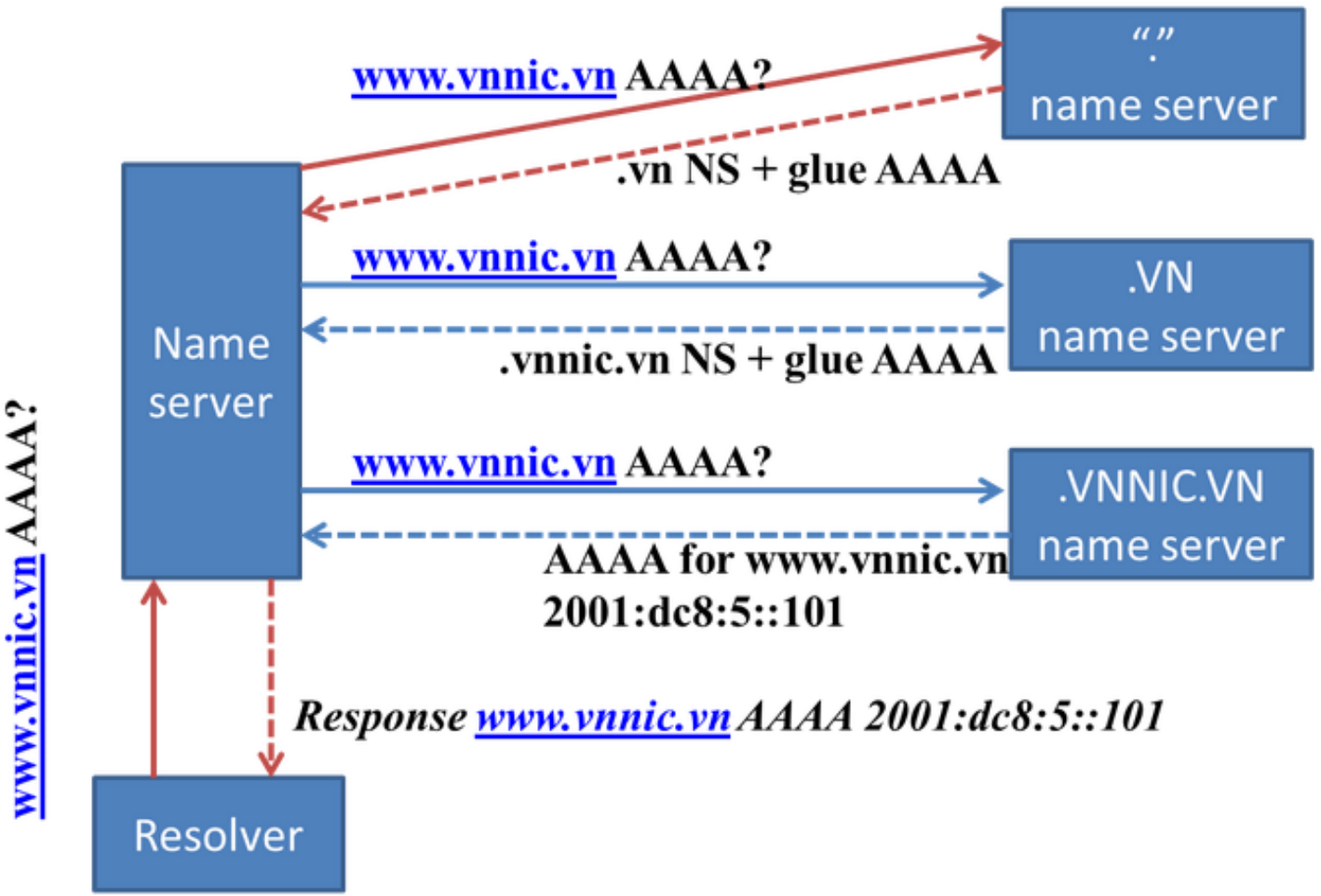
- Địa chỉ IPv6 hoàn toàn là dạng thức classless, không còn tồn tại khái niệm classfull. Địa chỉ IPv6 được biểu diễn gồm 32 chữ số hexa (mỗi số hexa tương ứng 4 bít). Tên miền ngược tương ứng địa chỉ IPv6 được chuyển giao theo các biên 4 bít đó.

# Các bản ghi tên miền

| | IPv4 | IPv6 |
|---|---|---|
| Bản ghi thuận | A | AAAA |
| Bản ghi ngược | - Tên miền: in-addr.arpa<br>- Chuyển giao dạng classfull (/8, /16, /24) | - Tên miền: ip6.arpa<br>- Chuyển giao theo các biên 4 bit (1 chữ hexa) |

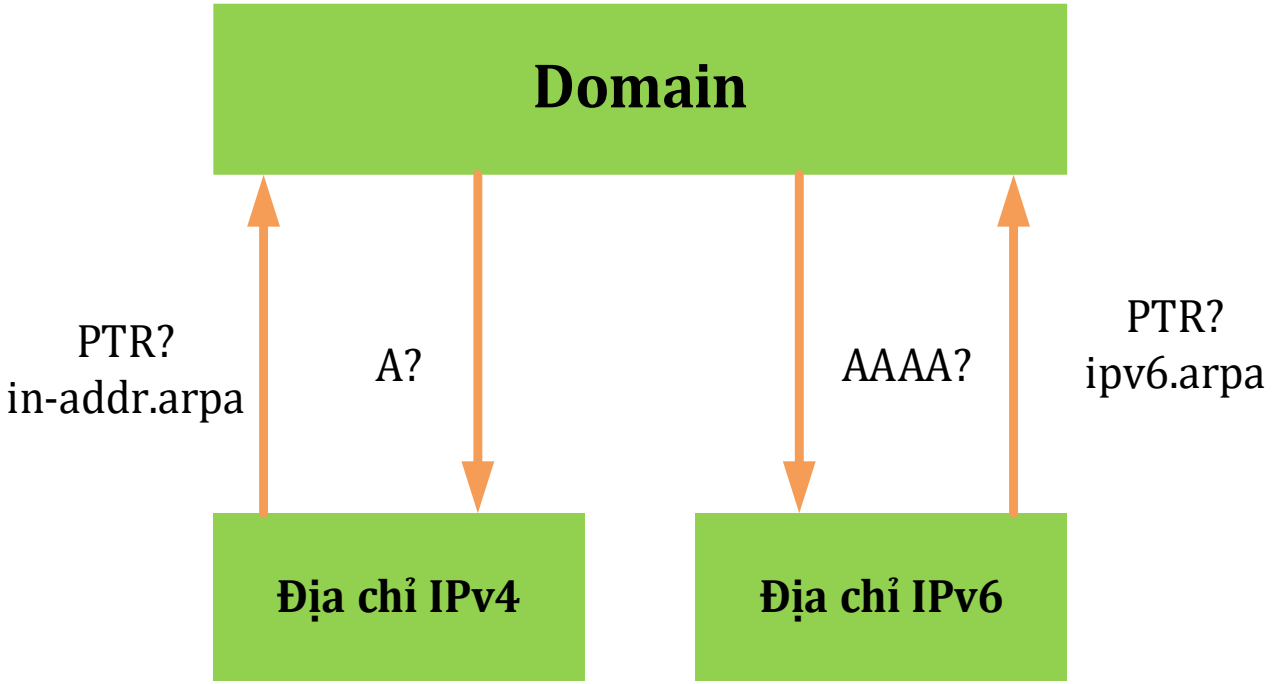


# Quá trình truy vấn, phân giải



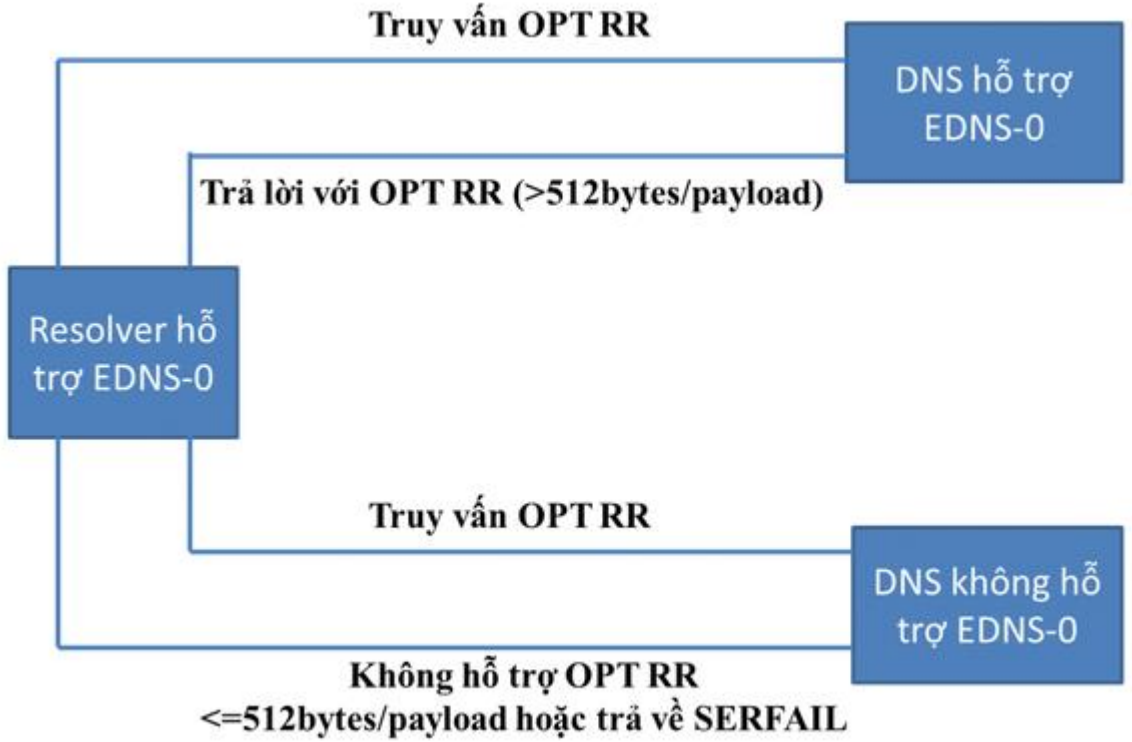
# Giao thức truyền tải

- Giao thức truyền tải DNS trong mạng IPv6 vẫn được giữ nguyên là UDP/53 và TCP/53.
- Quá trình truy vấn tên miền trong mạng thuần IPv6 hoàn toàn giống trong mạng IPv4
- Điểm khác biệt duy nhất ở đây là trường địa chỉ IP trong bản tin truy vấn và trả lời là địa chỉ IPv6 128 bít, điều này làm tăng tải xử lý và truyền dẫn trên mạng so với truy vấn địa chỉ IPv4.



# EDNS0

- UDP bị giới hạn 512 bytes, sử dụng TCP.
- Nếu quá nhiều TCP kết nối đến thì sẽ bị quá tải.
- RFC 2671 (ExtensionDNS, một Mechanisms for DNS EDNS0) đưa ra phương án giải quyết giới hạn 512 byte bằng cách bổ sung một bản ghi pseudo gọi là OPT.
- Nguyên tắc hoạt động là DNS Resolver và DNS server trao đổi thông tin về số lượng byte tối đa có thể sử dụng thông qua bản ghi OPT, từ đó có thể thực hiện các truy vấn quá 512 byte



# Thiết lập EDNS0

- Sử dụng tham số: edns-udp-size (bytes):
  - Thiết lập kích cỡ bộ đệm quảng bá EDNS UDP
  - Giá trị mặc định 4096.
- Thiết lập giá trị khác mặc định để câu trả lời UDP sẽ không bị firewall chặn các gói bị phân mảnh hoặc gói UDP lớn hơn 512 byte.

# Cấu hình IPv6

- Chạy TCP/IPv6 stack
- Mặc định BIND không chạy trên IPv6
- Thiết lập qua tham số trong option
  - options { listen-on-v6 { any; }; };
  - options { transfer-source-v6 222:10:2521:1:210:4bff:fe10:d24; };
  - options { notify-source-v6 222:10:2521:1:210:4bff:fe10:d24; };

# Khai báo bản ghi AAAA

- **Khai báo bản ghi AAAA:**

```
www     IN    A     192.168.0.3
mail    IN    A     192.168.0.32
www     IN    AAAA  2001:db8::3
mail    IN    AAAA  2001:db8::32
```

- **Kiểm tra các bản ghi AAAA:**

```
c:\bind>nslookup
> set type=aaaa
> vnnic.vn
Server:         203.119.11.211
Address:        203.119.11.211#53
Non-authoritative answer:
Name:   vnnic.vn
Address: 2001:dc8:0:2::93
```

# Khai báo bản ghi PTR

- **Ví dụ:**

```
; reverse IPV6 zone file for example.vn
$TTL 2d    ; default TTL for zone 172800 secs
$ORIGIN 0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA.
@       IN      SOA   ns1.example.vn. hostmaster.example.vn. (
                      2003080800 ; sn = serial number
                      12h        ; refresh = refresh
                      15m        ; retry = update retry
                      3w         ; expiry = expiry
                      2h         ; min = minimum
                      )
; name servers Resource Recordsfor the domain
        IN      NS      ns1.example.vn.
; the second name servers is
; external to this zone (domain).
        IN      NS      ns2.example.net.
; PTR RR maps a IPv6 address to a host name
; hosts in subnet ID 1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0      IN      PTR     ns1.example.vn.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0      IN      PTR     mail.example.vn.
; hosts in subnet ID 2
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0      IN      PTR     joe.example.vn.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0      IN      PTR     www.example.vn
```

# Phần mềm hỗ trợ

| Server | BSD | Solaris | Linux | Windows |
|---|---|---|---|---|
| BIND | Yes | Yes | Yes | Yes |
| Cisco Network Registrar | No | Yes | Yes | Yes |
| djbdns | Yes | Yes | Yes | No |
| Dnsmasq | Yes | Yes | Yes | No |
| gdnsd | Yes | Yes | Yes | No |
| Knot DNS | Yes | No | Yes | No |
| MaraDNS | Yes | Yes | Yes | Partial |
| Microsoft DNS | No | No | No | Included |
| Nominum ANS | Yes | Yes | Yes | No |
| Nominum Vantio | Yes | Yes | Yes | No |
| PowerDNS | Yes | Yes | Yes | Yes |
| Simple DNS Plus | No | No | No | Yes |

# Khuyến nghị cho DNS hoạt động IPv6

- Tổ chức, cá nhân khi triển khai DNS của mình trên mạng IPv6 cần tuân thủ theo hai RFC:
  - RFC 3901: “DNS IPv6 Transport Operational Guidelines”
  - RFC 4472: “Operational Considerations and Issues with IPv6”
- 02 RFC này hướng dẫn triển khai DNS và các vấn đề gặp phải trong quá trình triển khai, có thể tổng kết lại như sau:
  - Bất kỳ DNS zone nào nên được quản lý bởi ít nhất một DNS IPv4.
  - Các DNS đệ quy nên được triển khai trên mạng IPv4 hoặc dual-stack (cả IPv4 và IPv6).
  - Tất cả các zone nên được truy xuất qua cả mạng IPv4 và IPv6.

# Hướng dẫn triển khai DNS hoạt động IPv6 (1/2)

- **Yêu cầu:**
  - Hạ tầng mạng, máy chủ triển khai hỗ trợ IPv6
- **Hướng dẫn triển khai**
  - Bước 1: Thiết lập các cấu hình phần mềm DNS cho phép hoạt động trên IPv6
  - Bước 2: Khai báo thông tin bản ghi AAAA (IPv6) trong dữ liệu zone
  - Bước 3: Khai báo cập nhật thông tin AAAA (IPv6) của các máy chủ DNS lên zone tên miền cha (parent).
  - Bước 4: Kiểm tra hoạt động truy vấn qua IPv6

# Hướng dẫn triển khai DNS hoạt động IPv6 (2/2)

- Thiết lập qua tham số cho phép dịch vụ DNS hoạt động IPv6
  - options { listen-on-v6 { IPv6_Servers; }; };
  - options { transfer-source-v6 IPv6_Servers; };
  - options { notify-source-v6 IPv6_Servers; };

# Chuyển đổi Website IPv6

- Thuê dịch vụ NCC (Nhà cung cấp)
- Tự quản lý hệ thống máy chủ Webserver

# Chuyển đổi Website IPv6-Thuê dịch vụ NCC (1/2)

- Yêu cầu: Mạng lưới, hệ thống máy chủ dịch vụ của NCC đã hỗ trợ, hoạt động với IPv6.
- Kiểm tra kết quả kích hoạt IPv6 cho Website
  - Hướng dẫn kiểm tra bằng công cụ Online:

    Bước 1: Truy cập vào địa chỉ https://ipv6-test.com/

    Bước 2: Chọn mục Website trên thanh memu.

    Bước 3: Gõ tên miền tại mục tra cứu + nhấn enter (hoặc click vào Validate).

    Bước 4: Kiểm tra thông tin Website gồm (bản ghi AAAA của tên miền/website, IPv6 Web Server, DNS Server có thể IPv4 hoặc IPv6).

# Chuyển đổi Website IPv6-Thuê dịch vụ NCC (1/2)

- Gửi yêu cầu cho NCC triển khai IPv6 cho Website
  - Gửi yêu cầu cho NCC khai báo DNS và cài đặt, cấu hình IPv6 cho Website.
- Thực hiện gán nhãn IPv6 Ready Logo cho Website
  - Các cơ quan triển khai gán nhãn IPv6 Ready Logo cho Website theo hướng dẫn tại địa chỉ sau: http://vietnamipv6ready.vn/website.
- Thông báo kết quả cho VNNIC – Bộ TT&TT:
  - Sau khi hoàn tất kích hoạt hỗ trợ IPv6, các cơ quan gửi thông báo tới VNNIC qua địa chỉ: IPv6ForGov@vnnic.vn.
  - Danh sách website hoạt động & được gán nhãn IPv6 Ready Logo sẽ công bố trên Website Vietnam IPv6 Ready.

# Chuyển đổi Website IPv6-Tự quản lý hệ thống máy chủ Webserver (1/4)

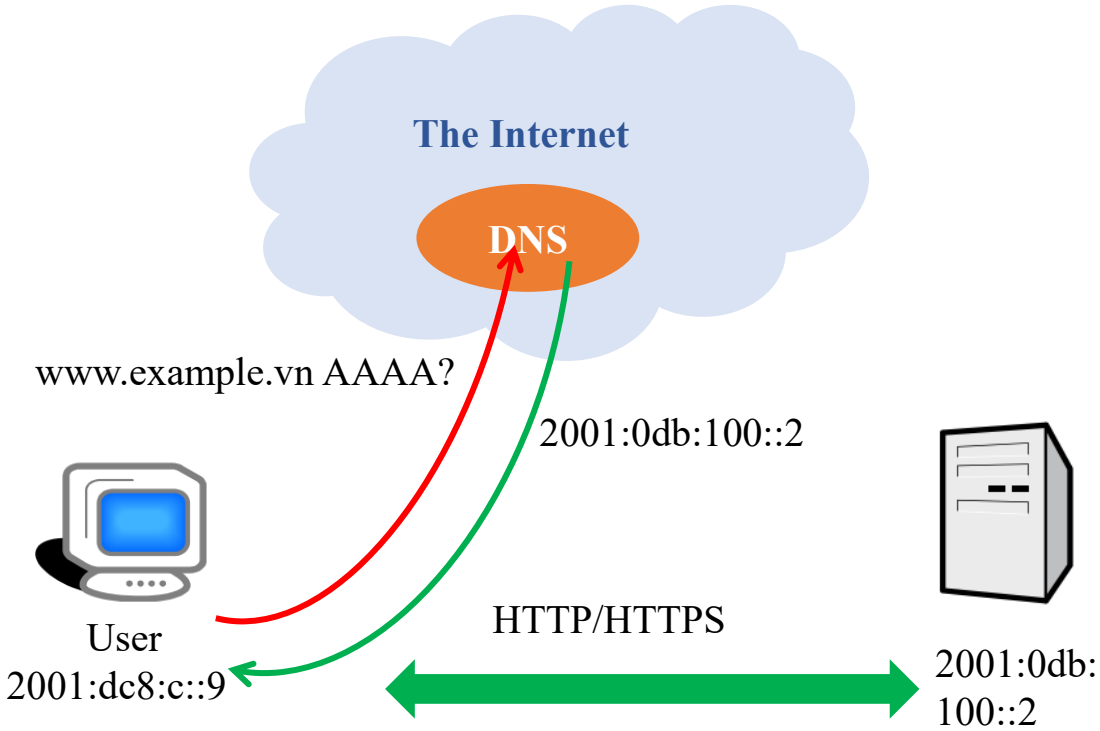
- **Yêu cầu:**
  - Mạng lưới, nơi đặt máy chủ Webserver đã triển khai và hoạt động với IPv6.
  - Máy chủ Web Server đã được triển khai IPv6.
- **Hướng dẫn triển khai Website IPv6:**

  Bước 1: Kích hoạt Web Server hỗ trợ IPv6.

  Bước 2: Trên DNS quản lý tên miền, khai báo bản ghi AAAA cho tên miền/website tương ứng trên hệ thống DNS.

  Bước 3: Kiểm tra kết quả

  Bước 4: Gán nhãn IPv6 ready logo.



# Chuyển đổi Website IPv6-Tự quản lý hệ thống máy chủ Webserver (2/4)

- Hướng dẫn các bước cài đặt, cấu hình IPv6 cho Website có thông tin như sau:
  - Tên miền cho website: www.example.vn
  - Địa chỉ IPv6 cho website: 2001:0db8:100::2
- Yêu cầu: Hạ tầng mạng, máy chủ đã hoạt động với IPv6
- Hướng dẫn thực hiện:

Bước 1: Cài đặt, cấu hình IPv6 cho ứng dụng Web Server (Apache Server, NGINX)

Bước 2: Trên DNS Hosting khai báo bản ghi IPv6 cho website:

www.example.vn IN AAAA 2001:0db8:100::2

# Chuyển đổi Website IPv6-Tự quản lý hệ thống máy chủ Webserver (3/4)

- **Apache Server:**
  - Kích hoạt web server hoạt động với IPv6 bằng sửa file cấu hình httpd.conf theo đường dẫn /etc/httpd/conf với nội dung như sau:

```
Listen [2001:0db8:100::2]:80
        <VirtualHost [2001:0db8:100::2]:80 >
                ServerName www.example.vn
                # ...
        </VirtualHost>
```

[Địa chỉ IPv6 của Website]: Cổng giao thức

Tên miền/ tên Website

  - Khởi động lại dịch vụ Apache Server

*# service httpd restart*

# Chuyển đổi Website IPv6-Tự quản lý hệ thống máy chủ Webserver (4/4)

- **Nginx Web Server:**
  - Kích hoạt web server hoạt động với IPv6 bằng sửa file cấu hình nginx.conf với nội dung như sau:

```
listen          [2001:0db8:100::2]:80;
server_name     www.example.vn;
```

[Địa chỉ IPv6 của Website]: Cổng giao thức

Tên miền/ tên Website

  - Khởi động lại dịch vụ Nginx Web Server

*# service nginx restart*

# VIII. DNSSEC

# Nội dung

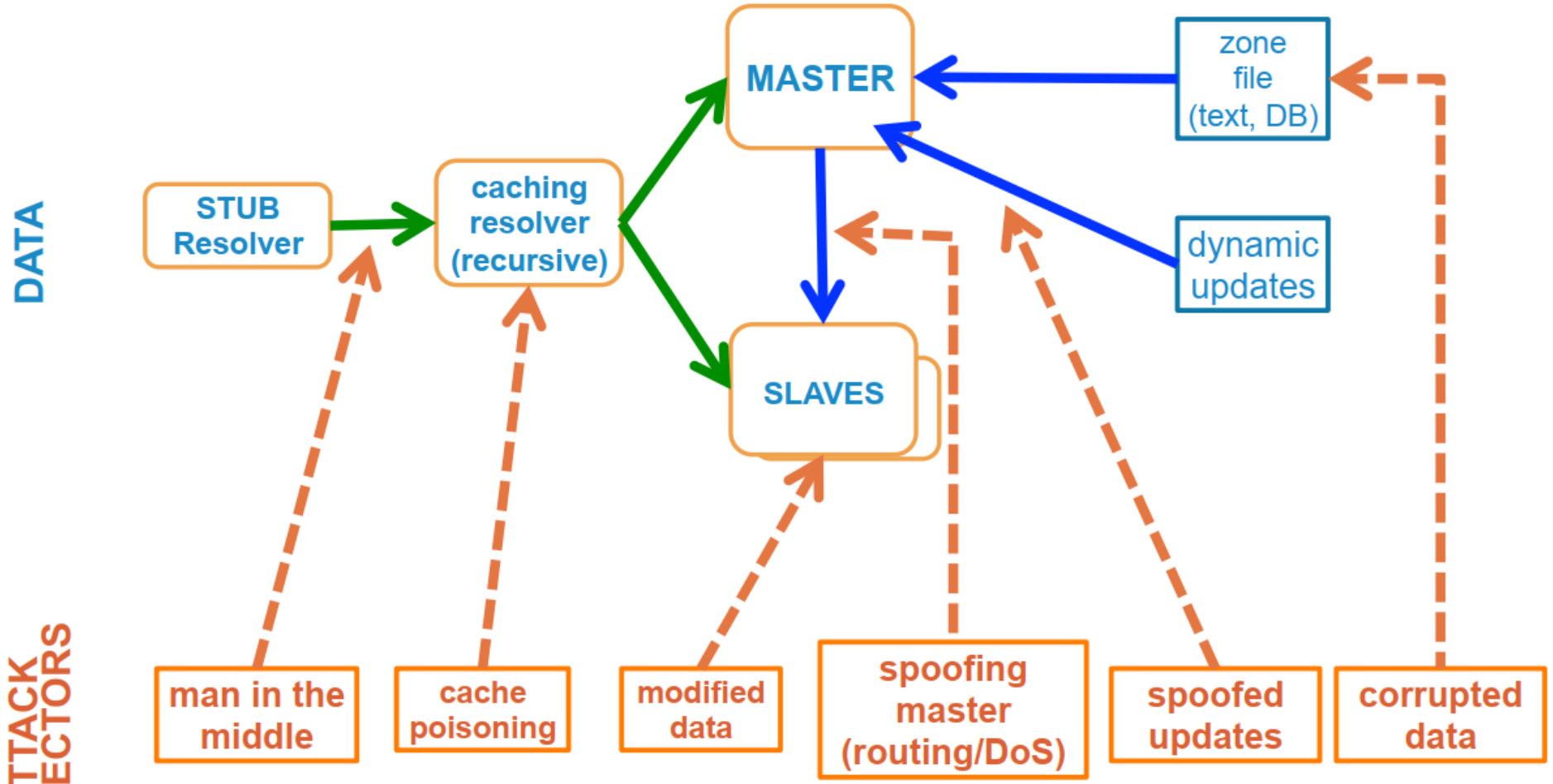
- Nguy cơ mất an toàn an ninh hệ thống DNS
  - Tấn công hệ thống DNS
  - DNS Cache Poisoning
  - Tấn công hệ thống DNS
  - DNSSEC ngăn chặn một số loại hình tấn công
- DNSSEC
  - Chức năng của DNSSEC
  - Hạ tầng mã hóa công khai PKI
  - Các bản ghi tài nguyên mới
  - Chain of Trust
- Triển khai DNSSEC
  - Các đối tượng triển khai DNSSEC
  - Mô hình triển khai DNSSEC
  - Triển khai DNSSEC cho CQNN

# Nguy cơ mất an toàn an ninh hệ thống DNS (1/2)

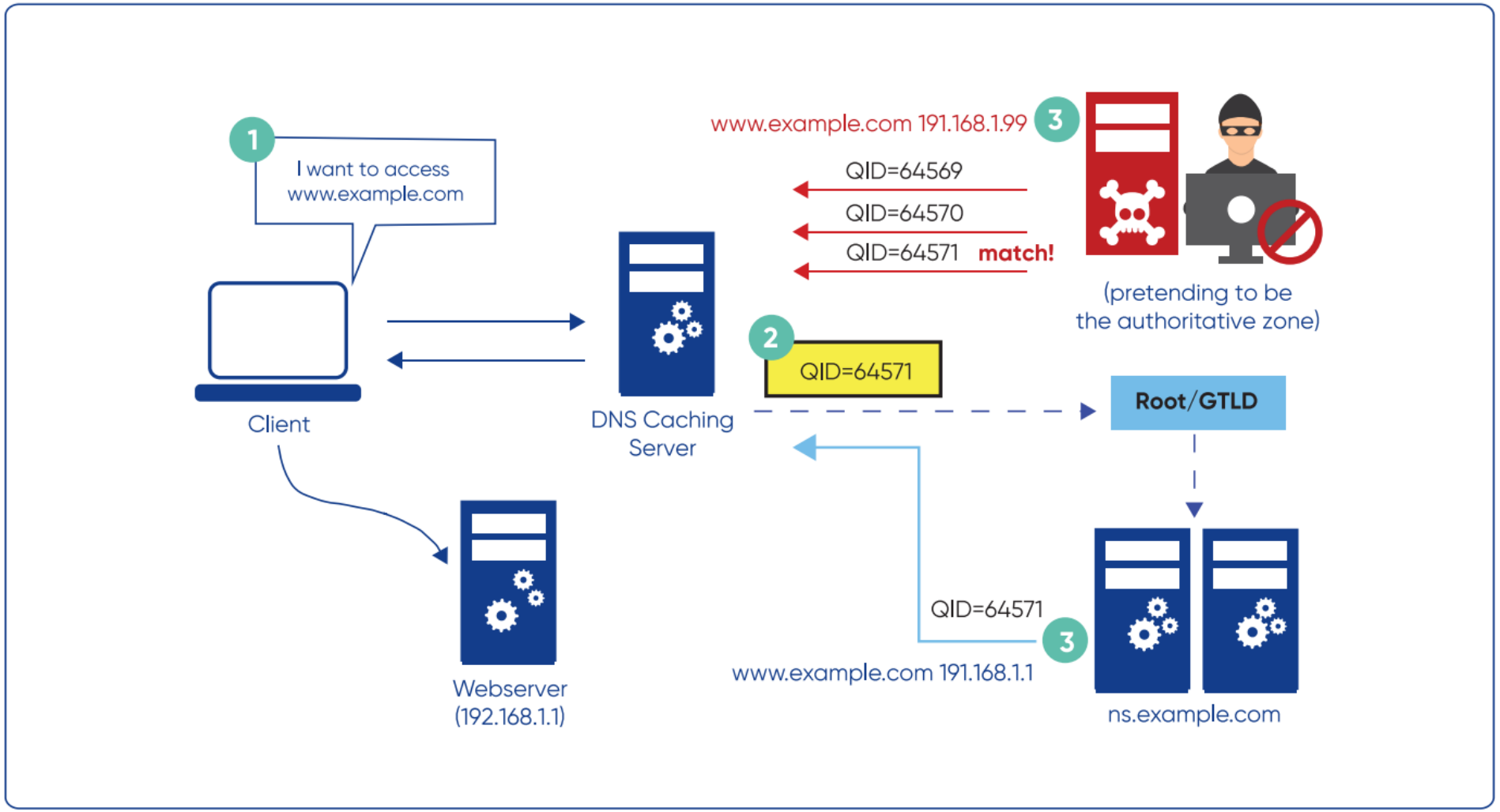
- DNS là hệ thống nền tảng quan trọng, giúp truy cập sử dụng dịch vụ trên Internet.
- DNS là mục tiêu của các cuộc tấn công nhằm chuyển hướng người dùng
- DNS sử dụng truyền tài UDP, bất kỳ gói tin UDP trả về chỉ cần đúng Source IP, Source Port, Destination IP, Destination Port, DNS query ID → Có thể vượt qua kiểm tra (bailiwick checking).
- Giao thức DNS ra đời từ lâu, giao thức DNS thông thường không có công cụ để xác thực nguồn dữ liệu.

→ Dữ liệu DNS có nguy cơ bị giả mạo và bị thay đổi trong quá trình trao đổi giữa các máy chủ DNS với các máy trạm (Resolver) hoặc máy chủ chuyển tiếp (Forwarder) → DNS Cache Poisoning.

# Nguy cơ mất an toàn an ninh hệ thống DNS (2/2)



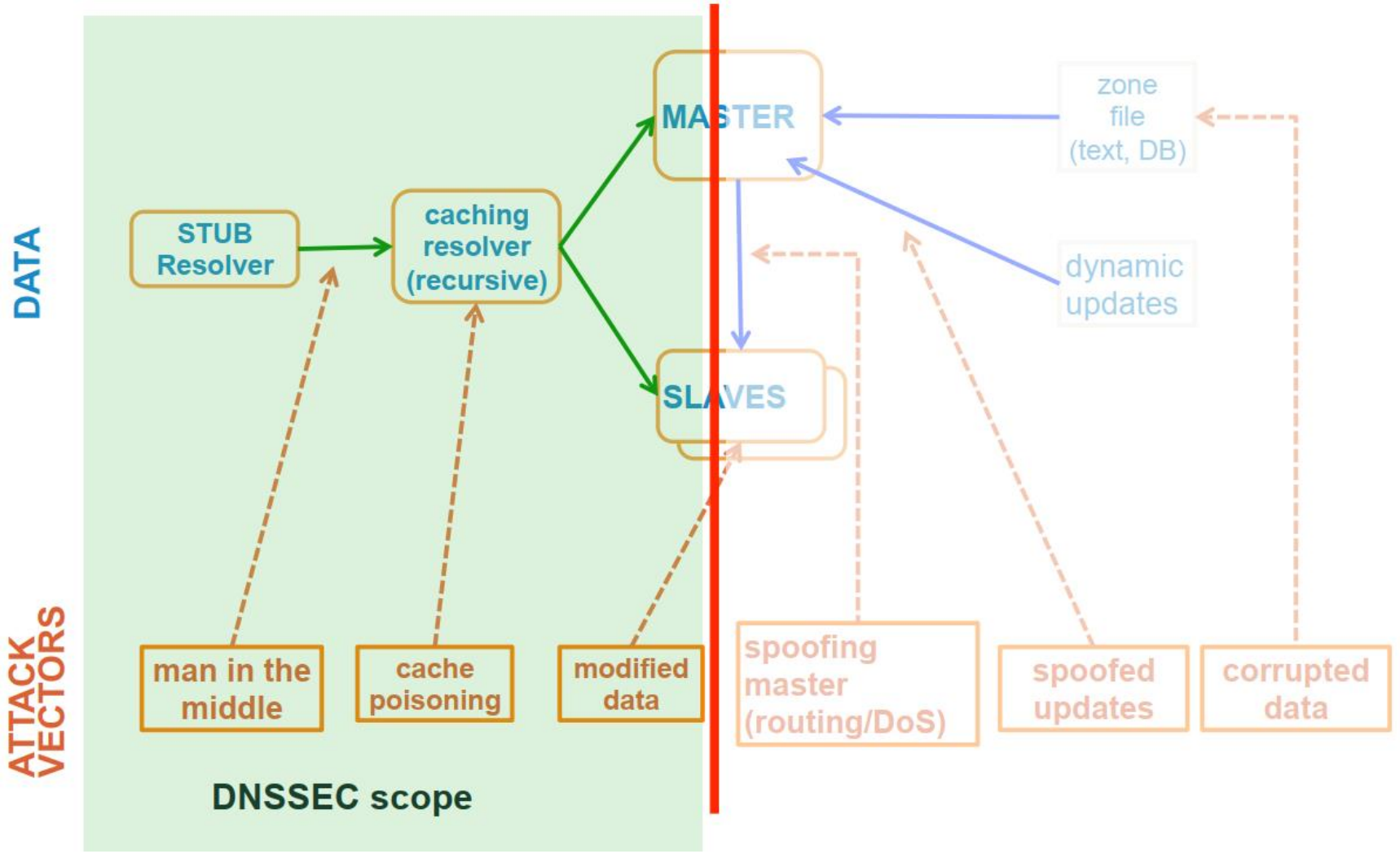
# DNS Cache Poisoning



# Tấn công hệ thống DNS

- Các dạng tấn công hệ thống DNS phổ biến bao gồm:
  - Tấn công sửa đổi dữ liệu DNS.
  - Tấn công giả mạo máy chủ DNS Master.
  - Tấn công làm nhiễm độc bộ nhớ Cache (DNS Cache Poisoning).
  - Tấn công Man-in-the-middle.

# DNSSEC ngăn chặn một số loại hình tấn công



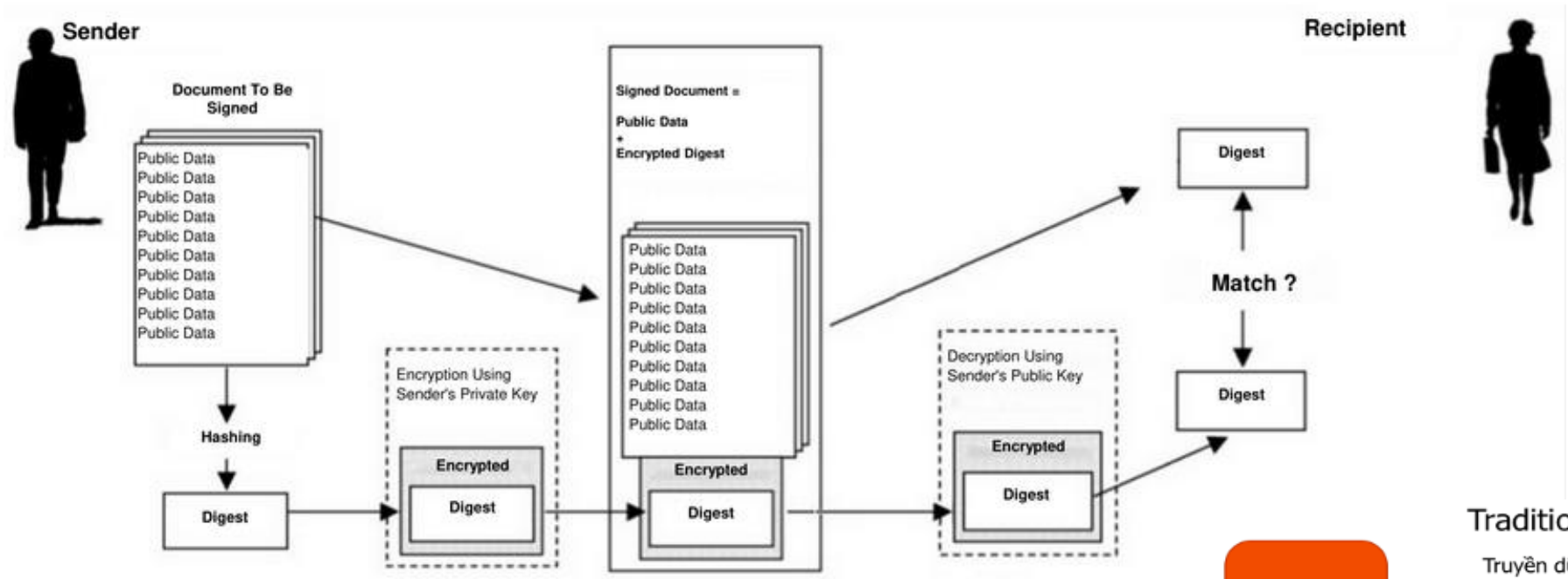
# DNSSEC

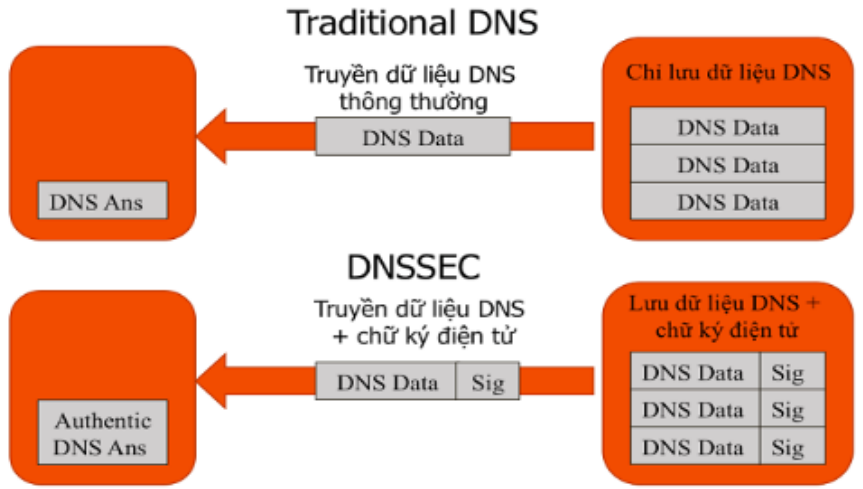
- DNSSEC (DNS Security Extensions) là tiêu chuẩn an toàn mở rộng của hệ thống DNS, được định nghĩa trong các RFC 4033, 4034, 4035.
- DNSSEC là công nghệ an toàn mở rộng của hệ thống DNS, DNSSEC không làm thay đổi cấu trúc và nền tang giao thức DNS, tiến trình truyền dữ liệu DNS và quá trình chuyển giao từ các DNS cấp cao xuống các DNS cấp thấp hơn (cùng tồn tại với hạ tầng hiện tại).
- Thay đổi mô hình DNS từ mô hình mở (open) sang mô hình tin cậy (trusting) và xác thực (verifiable). Người dùng Internet sử dụng DNSSEC được kiểm tra xác thực, toàn vẹn dữ liệu, đảm bảo truy cập an toàn.
- Sử dụng cơ sở hạ tầng mã hóa công khai PKI (private/public key).
- Thêm chữ ký số vào câu trả lời truy vấn

# Chức năng của DNSSEC

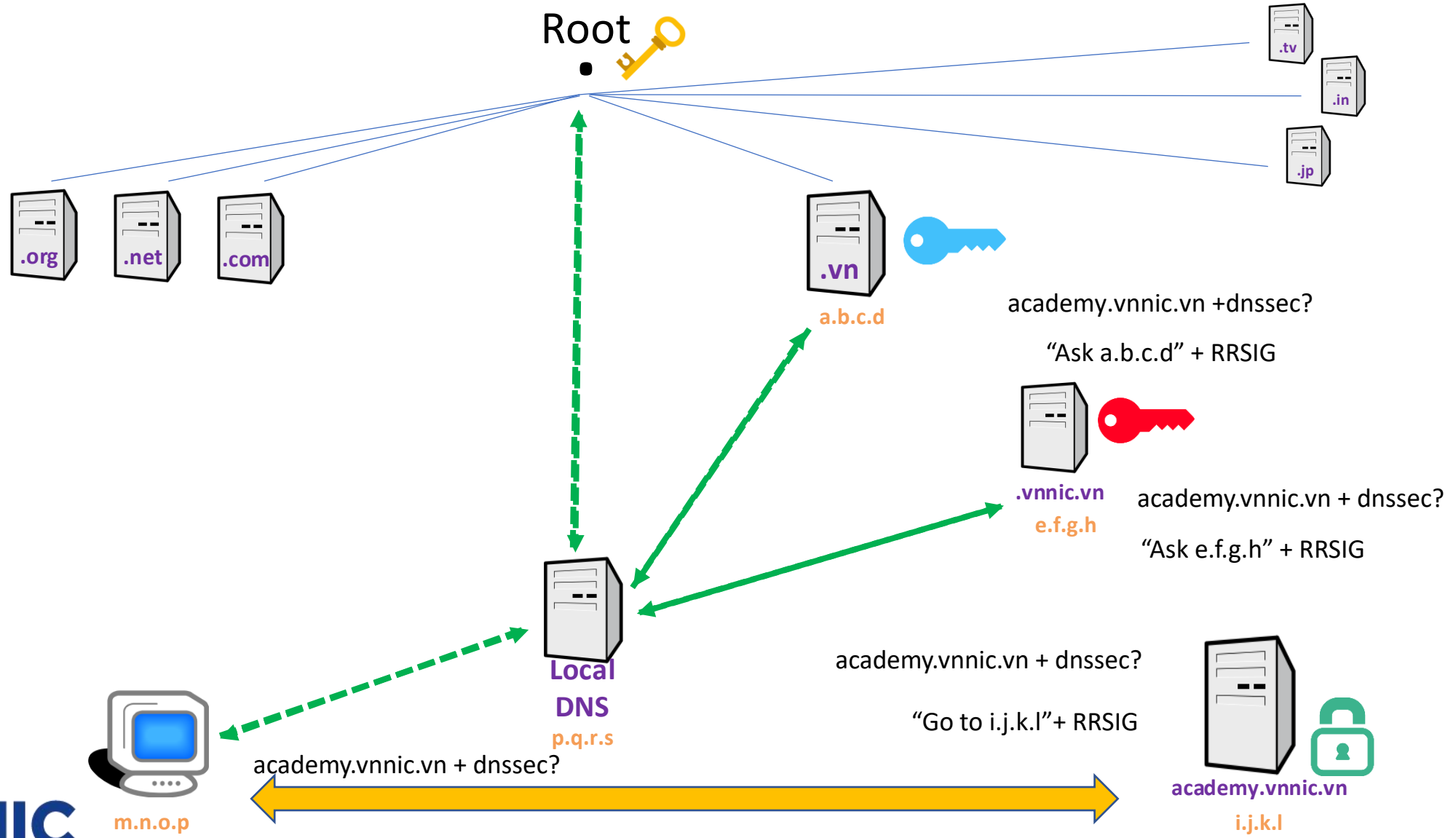
- DNSSEC ra đời nhằm các mục đích sau:
  - **Sender authentication:** Chứng thực nguồn gửi dữ liệu
  - **Data Integrity:** Toàn vẹn dữ liệu trong quá trình truyền
  - **Authenticated denial of existence:** Xác thực từ chối tồn tại (Ngăn chặn tấn công bằng cách tự động gửi xác nhận là không tồn tại dữ liệu mà client truy vấn)
  - DNSSEC không có tính năng Confidentiality (Mã hóa dữ liệu DNS)

# Hạ tầng mã hóa công khai PKI



# Qúa trình phân giải DNSSEC



# Vai trò của các máy chủ trong DNSSEC

- Các máy chủ DNS Authoritative
  - Ký DNSSEC cho các zone tên miền
  - Phản hồi các truy vấn được truy vấn đến đồng thời gửi kèm bản ghi chữ ký RRSIG trong phản hồi truy vấn
- Máy chủ xác thực (Validation Resolvers)
  - Xác thực các phản hồi truy vấn từ các máy chủ DNS
  - Dữ liệu không được xác thực hay xác thực thất bại sẽ có kết quả “SERVFAIL”

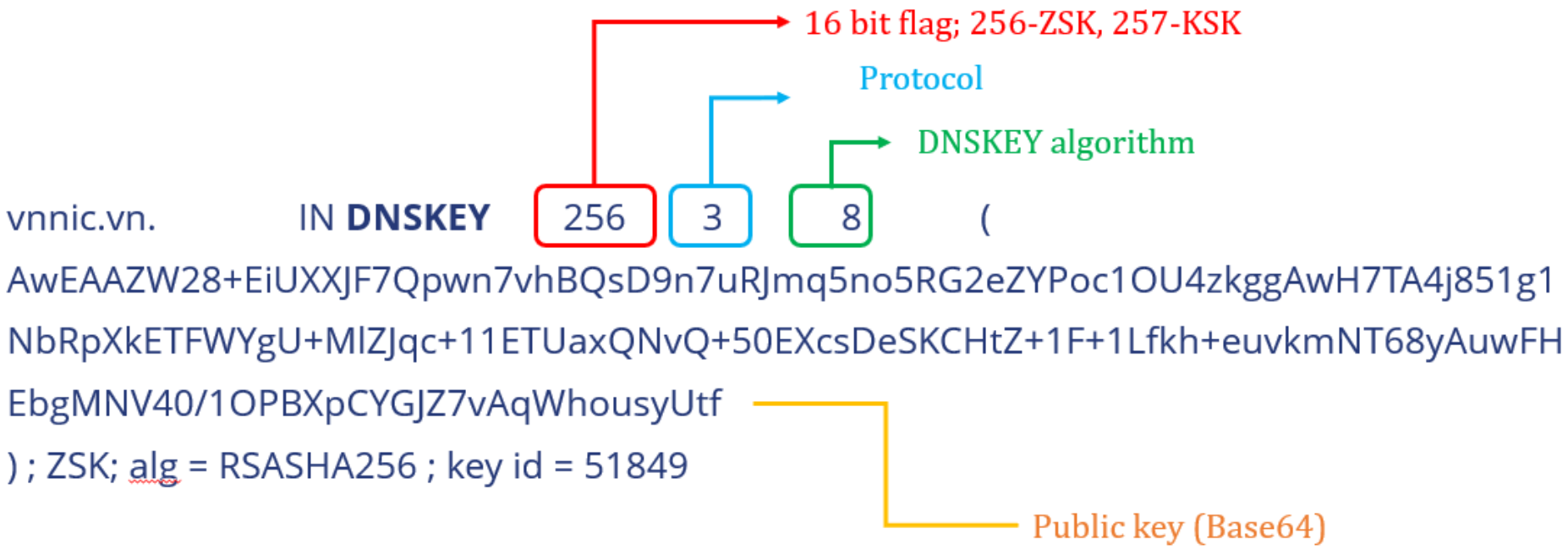
# Các bản ghi tài nguyên mới

Một zone dữ liệu được ký xác thực sẽ chứa đựng một trong các bản ghi RRSIG, DNSKEY, NSEC/NSEC3 và DS.

| Bản ghi | | Mô tả/ chức năng |
|---|---|---|
| **RRSIG** | Resource Record Signature | Bản ghi chữ ký tài nguyên, sử dụng để chứng thực cho các bản ghi tài nguyên trong zone dữ liệu. |
| **DNSKEY** | DNS Key | Bản ghi khóa công cộng DNS, sử dụng để xác thực bản ghi RRSIG |
| **DS** | Delegation Signer | Bản ghi ký ủy quyền, sử dụng xác thực chuyển giao DNS. |
| **NSEC / NSEC3** | Next Secure | Bản ghi bảo mật kế tiếp, xác định các tên miền tiếp theo trong zone, mục đích xác thực từ chối sự tồn tại của các tên miền không tồn tại. |

# Bản ghi DNSKEY (1/3)

- Chứa thông tin khóa công khai của Zone
- Sử dụng để ký và xác thực các bản ghi tài nguyen trong zone
- Ví dụ:



# Bản ghi DNSKEY (2/3)

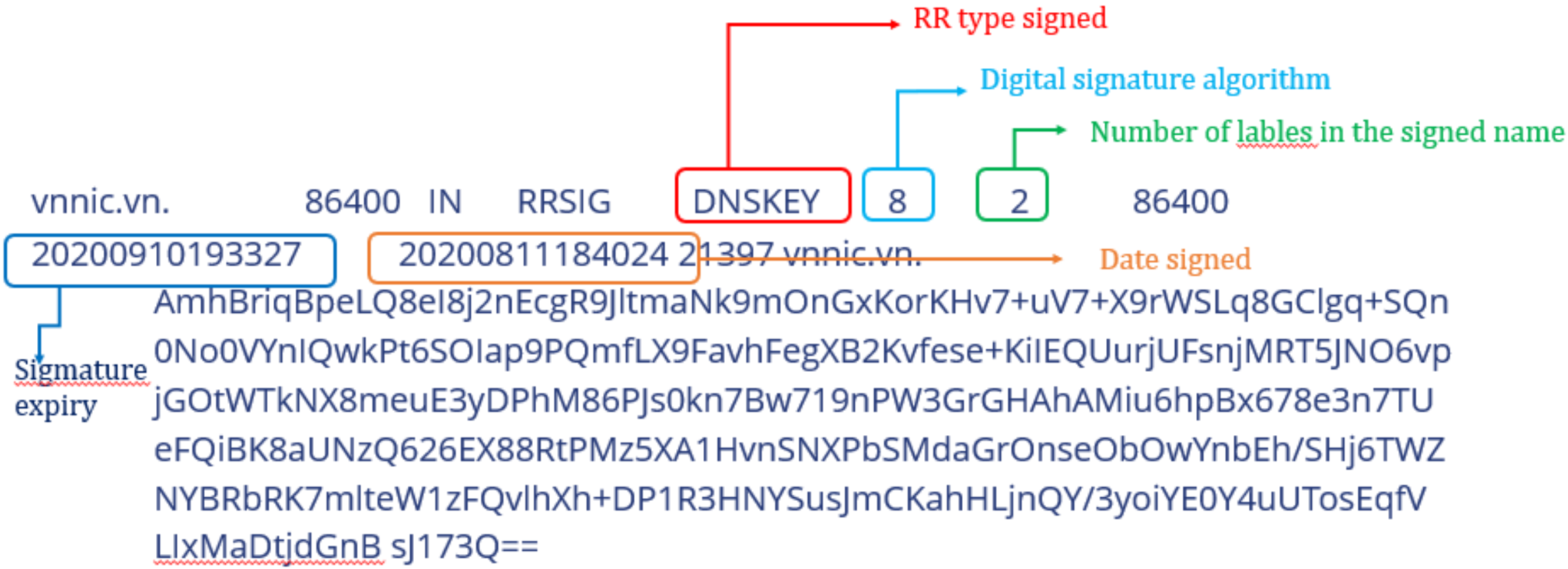
- Trong mỗi zone có ít nhất 02 bản ghi DNSKEY
- DNSKEY được tạo bởi từ một cặp khóa (public, private) sử dụng để ký cho zone:
  - Private: khóa sử dụng để ký dữ liệu zone (các bản ghi tài nguyên RRsets)
  - Public: khóa công khai, public trong zone (DNSKEY)

# Bản ghi DNSKEY (3/3)

- KSK và ZSK
  - Zone Signing Key (ZSK) được sử dụng để ký cho tất cả các dữ liệu thẩm quyền trong một zone.
  - Key Signing Key (KSK) được dùng để ký bản ghi DNSKEY trong một zone.

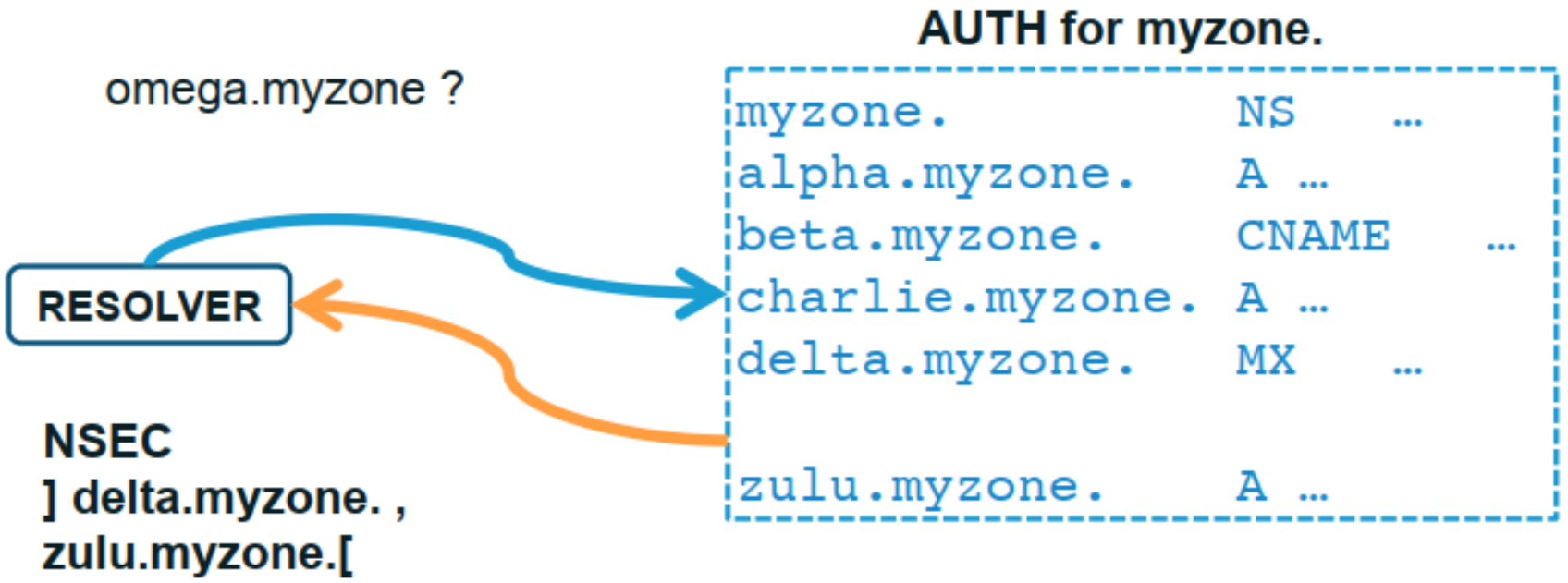
| KSK | ZSK |
|---|---|
| - KSK dùng để ký bản ghi DNSKEY trong một zone.<br><br>- KSK luôn có odd flag là 257.<br><br>- Khi KSK thay đổi, bản ghi DS trong parent zone phải được update.<br><br>- KSK thường được tạo với kích thước lớn để chống lại các tấn công brute force.<br><br>- KSK thường có thời gian sống (lifetime) lâu | - ZSK đqợc dùng để ký cho tất cả các bản ghi trong zone (bao gồm cả DNSKEY). Tuy nhiên không ký cho các bản ghi NS chuyển giao và glue records.<br><br>- ZSK luôn có odd flag là 256.<br><br>- Khi ZSK thay đổi, không cần thiết phải thay đổi bản ghi DS trên parent zone.<br><br>- ZSK thường có thời gian sống ngắn hơn, và được “rolled” nhiều hơn. |

# Bản ghi RRSIG



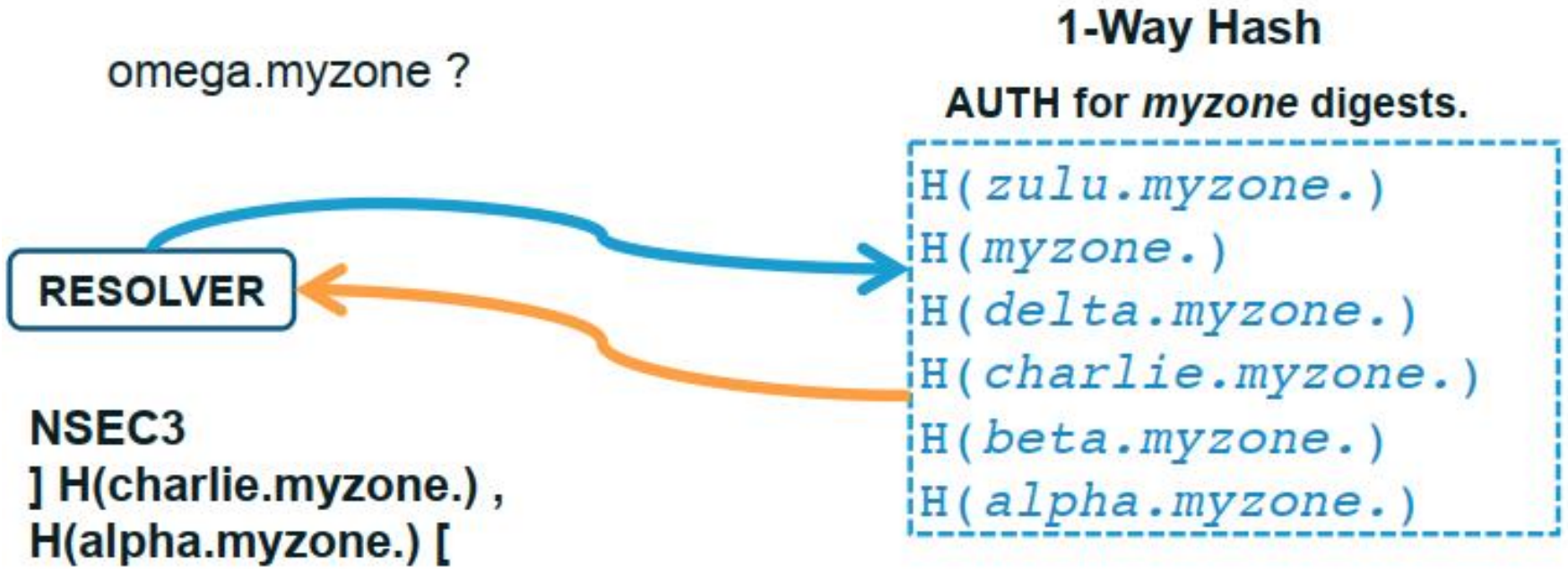
# Bản ghi NSEC (Next Secure) (1/2)

- Tạo thành một chuỗi các tên miền kế tiếp nhau trong zone
- Xác thực từ chối sự tồn tại của các tên miền NXDomains (không tồn tại)



# Bản ghi NSEC3 (2/2)

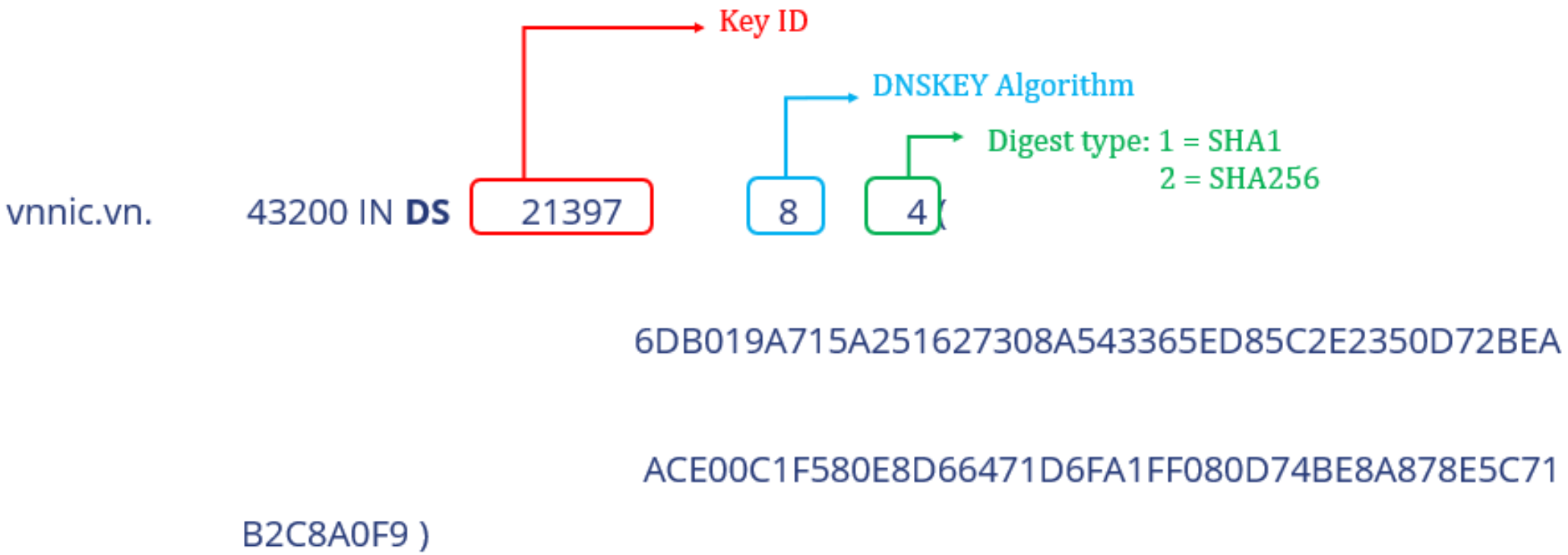
- Có chức năng tương tự NSEC và cung cấp cơ chế bảo mật hơn
- Chống lại các dạng tấn công liệt kê danh sách tên miền “zone walking”



# Bản ghi DS (Delegation Signer) (1/2)

- DS-Delegation Signer, bản ghi ký chuyển giao dùng để xác thực quá trình chuyển giao của parent zone và child zone.
- Bản ghi DS được sử dụng trong quá trình xác thực DNSKEY. Trả lời cho câu hỏi: Public key của zone có hợp lệ hay không hợp lệ?
- DS chính là giá trị hash khóa KSK trong bản ghi DNSKEY của child zone.
- DS được lưu trữ trong parent zone, cùng với các bản ghi NS chuyển giao của child zone.
- Bản ghi DS của child zone được ký cùng với phần còn lại của dữ liệu parent zone.

# Bản ghi DS (Delegation Signer) (1/2)

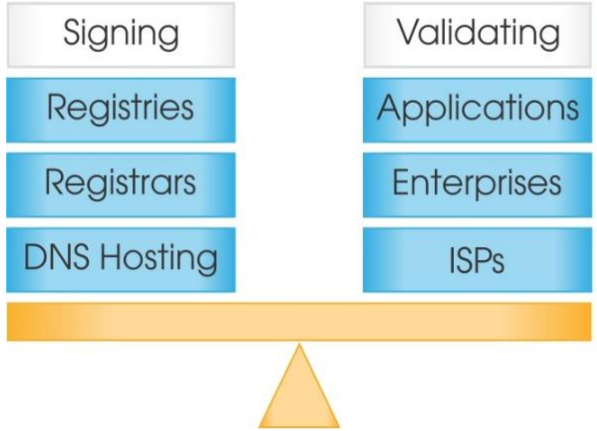


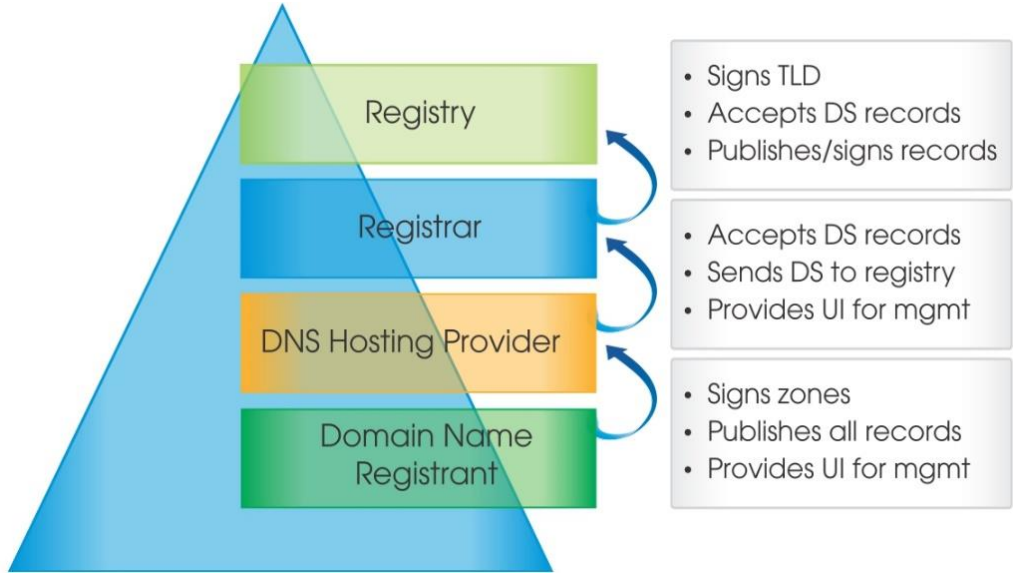
# Chain of Trust

- Là xác lập một chuỗi tin tưởng trong DNSSEC, bắt đầu từ root đến zone được ký, mỗi thành phần trong chuỗi trong liên kết được validate với thành phần kế tiếp nó.
  - Bản ghi DS trong parent được sử dụng để xác thực public key (DNSKEY) của child.

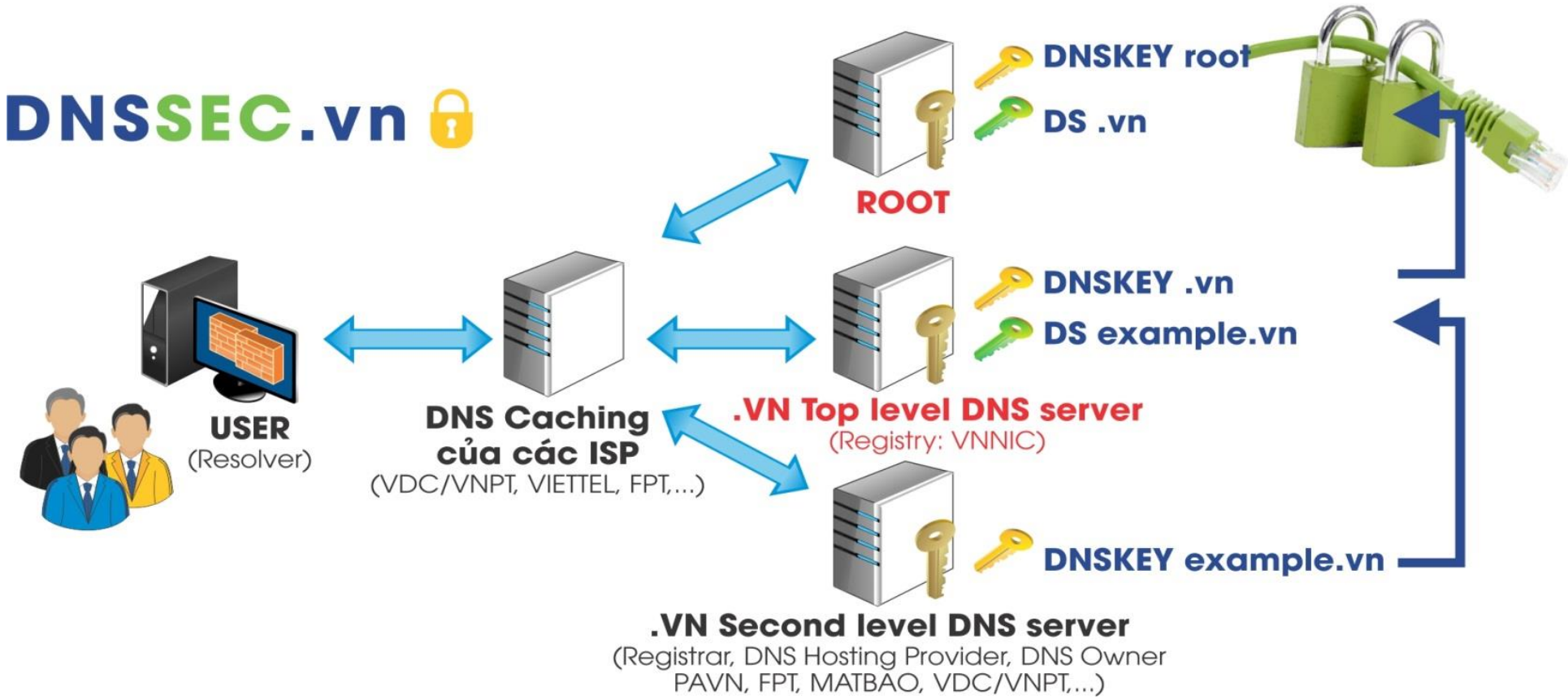
# Các đối tượng triển khai DNSSEC

- **2 nhóm đối tượng chính**
  - Nhóm ký số dữ liệu tên miền bao gồm: DNS Authoritative (Registries, Registrars, DNS Hosting)
  - Nhóm kiểm tra dữ liệu tên miền: DNS Cache (các ISP, các ứng dụng, các Enterprises)



# Mô hình triển khai DNSSEC




- Triển khai: ROOT → DNS TLD → DNS cấp dưới(IPS/Registar/DNS Hosting/Ower)

# Triển khai DNSSEC

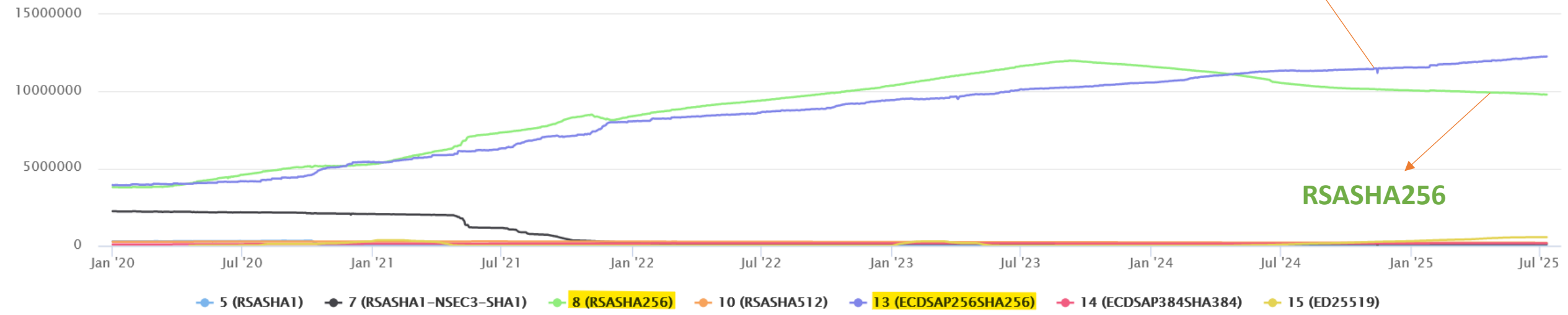
- **DNS Authoritative**:
  - Nâng cấp hệ thống DNS hỗ trợ DNSSEC.
  - Tạo khóa, ký số tên miền
- **DNS Cache:**
  - Không ký số tên miền (trừ các tên miền tự quản lý)
  - Xác thực DNSSEC: Bật chế độ DNSSEC validation trong các phần mềm DNS có sẵn

# Xu hướng tham số DNSSEC

KSK ALGORITHM | ZSK ALGORITHM | RSA KSK SIZES | RSA ZSK SIZES | RSA EXPONENTS

DNSKEY parameter frequency (1000 or more instances), by zone count:

**Historical trend**



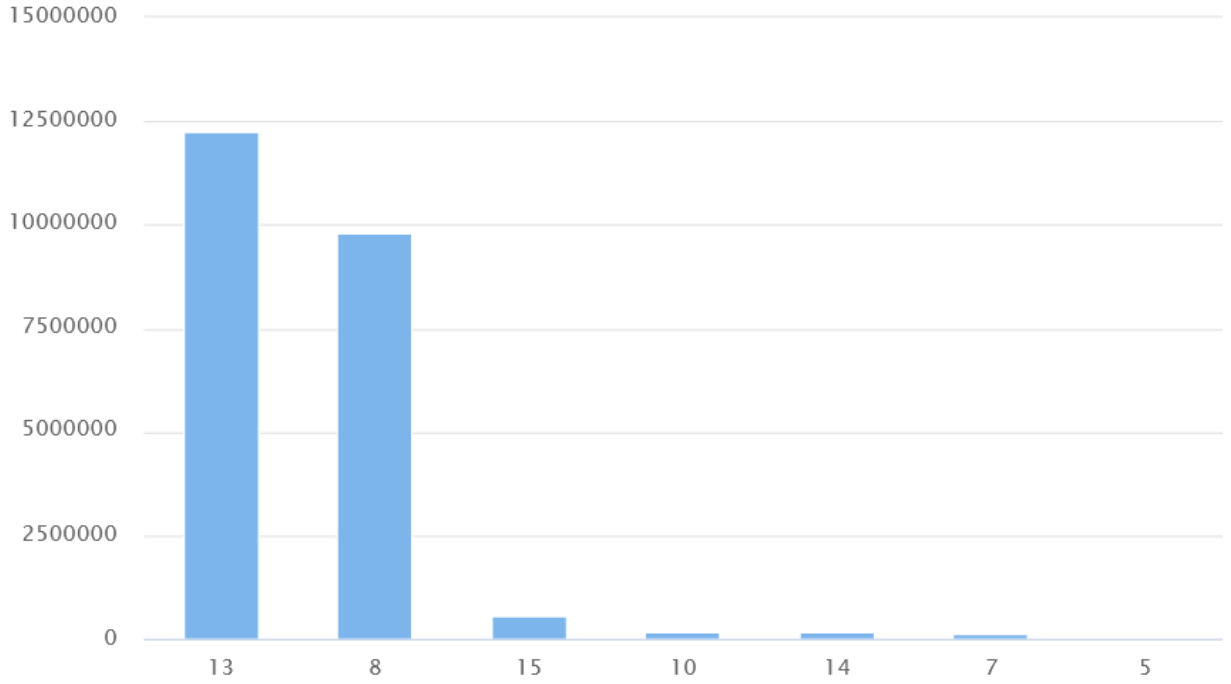

ECDSAP256SHA256

RSASHA256

# Xu hướng tham số DNSSEC

Today's Values

| KSK Algorithm | Flags | Protocol | Domain Count |
|---|---|---|---|
| 5 | 257 | 3 | 17963 |
| 7 | 257 | 3 | 111011 |
| 8 | 257 | 3 | 9801137 |
| 10 | 257 | 3 | 191540 |
| 13 | 257 | 3 | 12263361 |
| 14 | 257 | 3 | 156785 |
| 15 | 257 | 3 | 559500 |

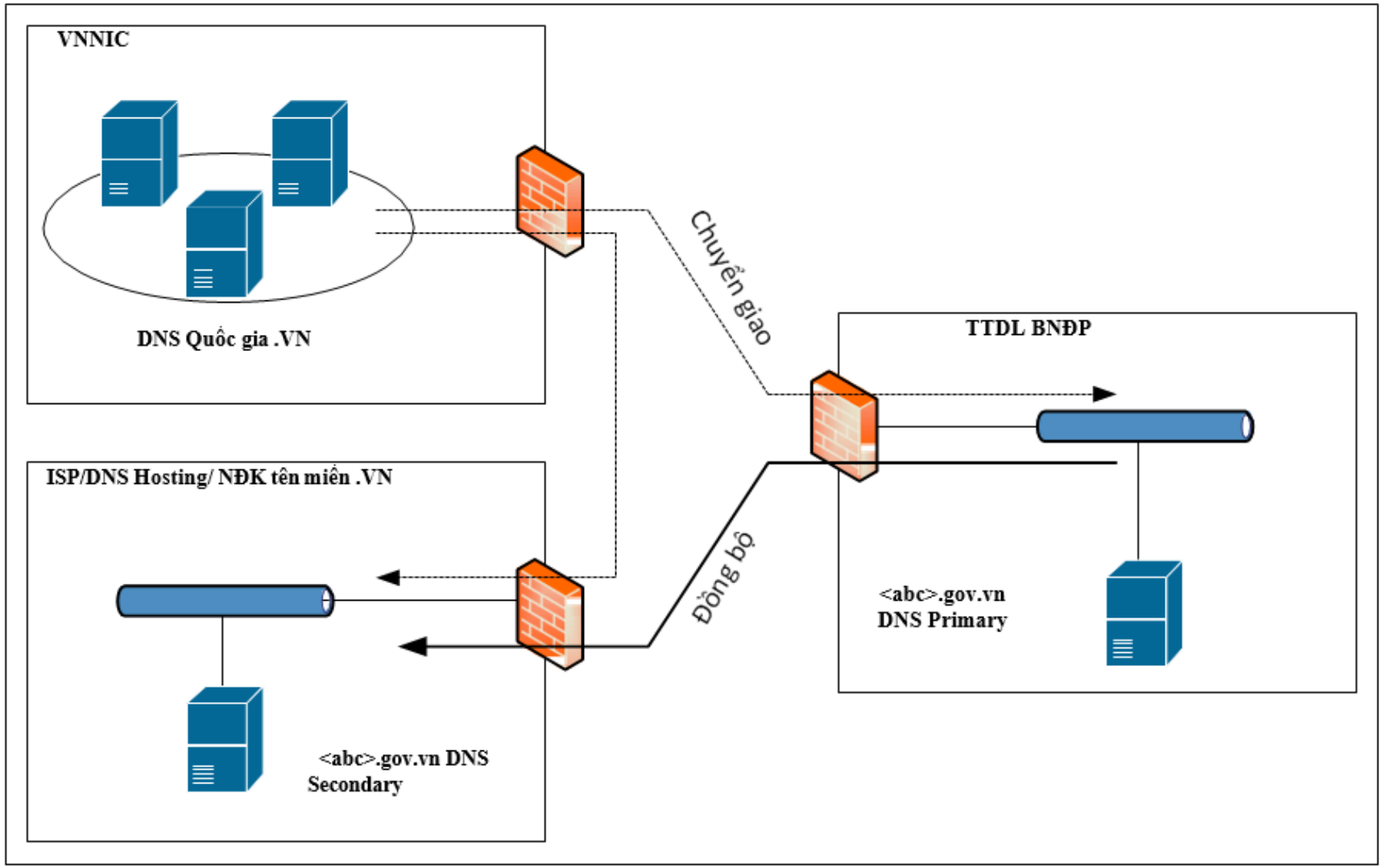


# THỰC HÀNH

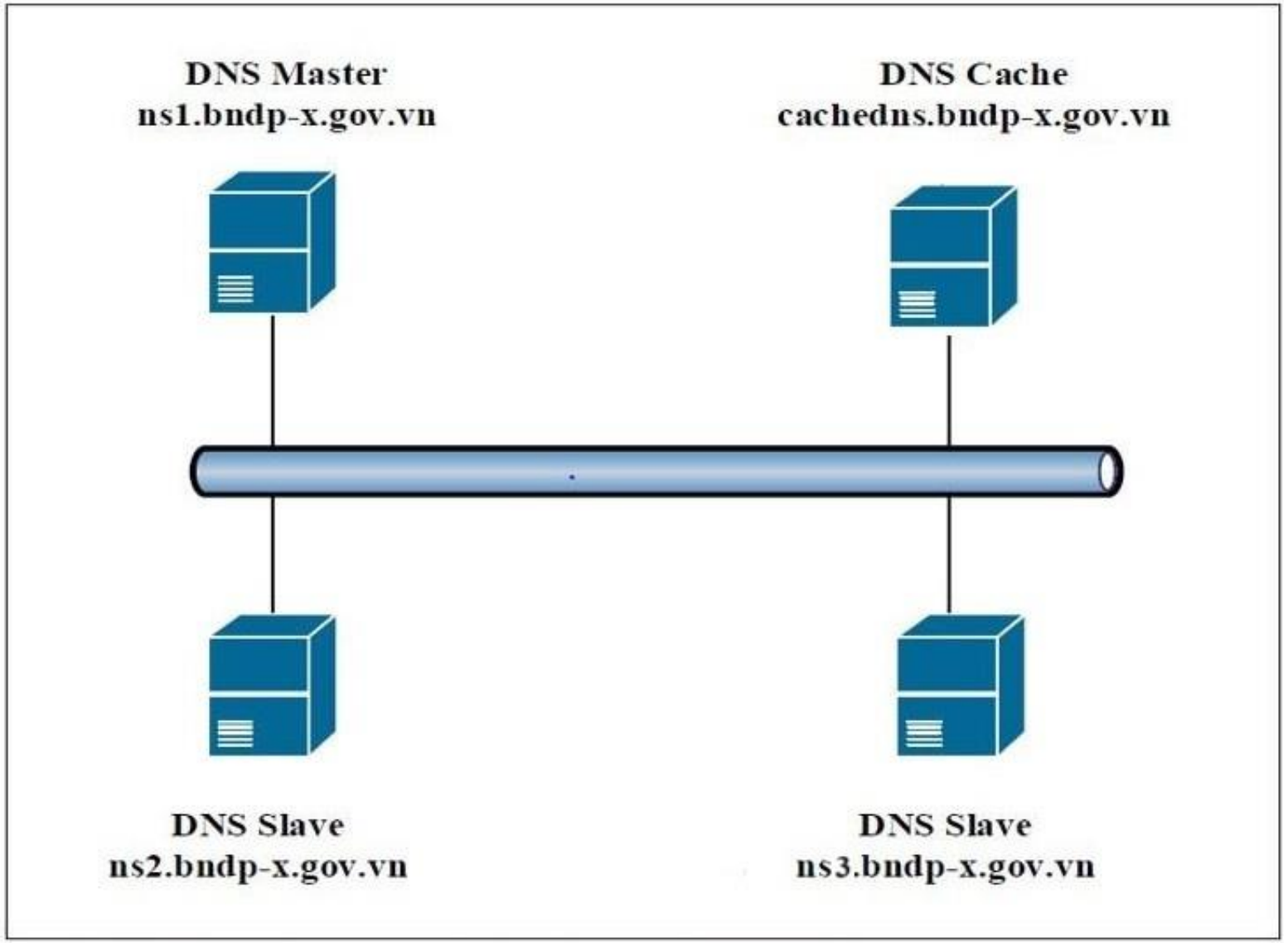
# THỰC HÀNH DNS

- Mô hình thực hành
- Kịch bản thực hành

# Mô hình tổng quan
# Hệ thống DNS quản lý tên miền .gov.vn



# Mô hình thực hành
# Hệ thống DNS quản lý tên miền và DNS Cache



# Kịch bản thực hành

- **Bài thực hành 1:** Thực hành triển khai hệ thống DNS cơ bản
  - Triển khai DNS Authoritative hoạt động theo mô hình Master-Slave
  - Triển khai máy chủ DNS Cache
- **Bài thực hành 2:** Thực hành triển khai tối ưu và gỡ lỗi hệ thống DNS
  - Cấu hình đồng bộ dữ liệu sử dụng TSIG
  - Thiết lập RNDC
- **Bài thực hành 3:** Thực hành chuyển đổi IPv6 cho DNS
  - Thiết lập máy chủ DNS hoạt động IPv6
  - Thiết lập dịch vụ DNS hoạt động IPv6
- **Bài thực hành 4:** Thực hành triển khai DNSSEC
  - Thiết lập ký DNSSEC
  - Thiết lập chuỗi xác thực DNSSEC

# Trao đổi, bài học

VNNIC
Internet for all

.vn TÊN MIỀN QUỐC GIA VIỆT NAM

VNIX
Viet Nam National Internet eXchange

DNS
National .VN Domain Name System

ASN
Your Net ID

INTERNET SPEED by VNNIC

IP
v4 v6
Internet Address

VNIXNOG
VietNam National Internet eXchange
Network Operators Group

VNNIC
INTERNET CONFERENCE

VNNIC
INTERNET ACADEMY

VNNIC
INTERNET ATLAS

Xin trân trọng cám ơn !


BỘ KHOA HỌC VÀ CÔNG NGHỆ - TRUNG TÂM INTERNET VIỆT NAM

**TP. Hà Nội:** Tầng 24, Toà nhà VNTA, Dương Đình Nghệ, Yên Hoà, Cầu Giấy, Hà Nội

**TP. Đà Nẵng:** Lô 21, Đường số 7, KCN An Đồn, Sơn Trà, Đà Nẵng

**TP. Hồ Chí Minh:** Đường số 20, Khu chế xuất Tân Thuận, Quận 7, TP. Hồ Chí Minh

+84 24 3556 4944

webmaster@vnnic.vn

facebook.com/myVNNIC/

https://vnnic.vn/