



BỘ THÔNG TIN VÀ TRUYỀN THÔNG  
TRUNG TÂM INTERNET VIỆT NAM

# XÂY DỰNG VÀ VẬN HÀNH HỆ THỐNG DNS CHO CQNN

Email: [ipv6forgov@vnnic.vn](mailto:ipv6forgov@vnnic.vn)

Web: <https://vnnic.vn/ipv6forgov>

# NỘI DUNG

## ❖ Phần I: Hệ thống DNS

- ✓ Lý thuyết hệ thống DNS
- ✓ DNS hoạt động IPv6
- ✓ DNSSEC
- ✓ Xác thực thư điện tử dựa trên DNS

## ❖ Phần II: Khuyến nghị hệ thống DNS cho các CQNN

- ✓ Khuyến nghị cho DNS Authoritative
- ✓ Khuyến nghị cho DNS Cache
- ✓ Xác thực thư điện tử Email Authentication

## ❖ Phần III: Thực hành DNS

- ✓ Cài đặt, cấu hình dịch vụ DNS
- ✓ Chuyển đổi IPv6 cho hệ thống DNS và Website
- ✓ Triển khai DNSSEC
- ✓ Xác thực thư điện tử Email Authentication

# PHẦN I: HỆ THỐNG DNS

## ➤ 1.1. Lý thuyết hệ thống DNS

- ✓ Hệ thống DNS là gì?
- ✓ Các loại máy chủ DNS
- ✓ File dữ liệu và bản ghi tên miền
- ✓ Hoạt động của hệ thống DNS
- ✓ Cài đặt và cấu hình hệ thống DNS
- ✓ Quản trị và gỡ lỗi DNS
- ✓ An toàn và tối ưu hệ thống DNS

## ➤ 1.2. DNS hoạt động IPv6

- ✓ Quá trình truy vấn, phân giải
- ✓ Khuyến nghị cho DNS hoạt động IPv6
- ✓ Hướng dẫn triển khai DNS hoạt động IPv6
- ✓ Chuyển đổi Website IPv6
- ✓ Khuyến nghị triển khai

## ➤ 1.3. DNSSEC

- ✓ Nguy cơ an toàn an ninh hệ thống DNS
- ✓ Tấn công hệ thống DNS
- ✓ DNSSEC
- ✓ DNSSEC hoạt động như thế nào?
- ✓ Hoạt động truy vấn DNSSEC
- ✓ Các bản ghi tài nguyên mới
- ✓ Chain of Trust
- ✓ Triển khai DNSSEC trên hệ thống DNS Root

## ➤ 1.4. Xác thực thư điện tử Email Authentication

- ✓ Hệ thống thư điện tử (Email)
- ✓ Các mối đe dọa trong giao thư điện tử
- ✓ Email Authentication
- ✓ Giải pháp SPF
- ✓ Giải pháp DKIM
- ✓ Giải pháp DMARC

# PHẦN I: HỆ THỐNG DNS

## ➤ 1.1. Lý thuyết hệ thống DNS

- ✓ Hệ thống DNS là gì?
- ✓ Các loại máy chủ DNS
- ✓ File dữ liệu và bản ghi tên miền
- ✓ Hoạt động của hệ thống DNS
- ✓ Cài đặt và cấu hình hệ thống DNS
- ✓ Quản trị và gỡ lỗi DNS
- ✓ An toàn và tối ưu hệ thống DNS

## ➤ 1.2. DNS hoạt động IPv6

- ✓ Quá trình truy vấn, phân giải
- ✓ Khuyến nghị cho DNS hoạt động IPv6
- ✓ Hướng dẫn triển khai DNS hoạt động IPv6
- ✓ Chuyển đổi Website IPv6
- ✓ Khuyến nghị triển khai

## ➤ 1.3. DNSSEC

- ✓ Nguyên tắc an toàn an ninh hệ thống DNS
- ✓ Tấn công hệ thống DNS
- ✓ DNSSEC
- ✓ DNSSEC hoạt động như thế nào?
- ✓ Hoạt động truy vấn DNSSEC
- ✓ Các bản ghi tài nguyên mới
- ✓ Chain of Trust
- ✓ Triển khai DNSSEC trên hệ thống DNS Root

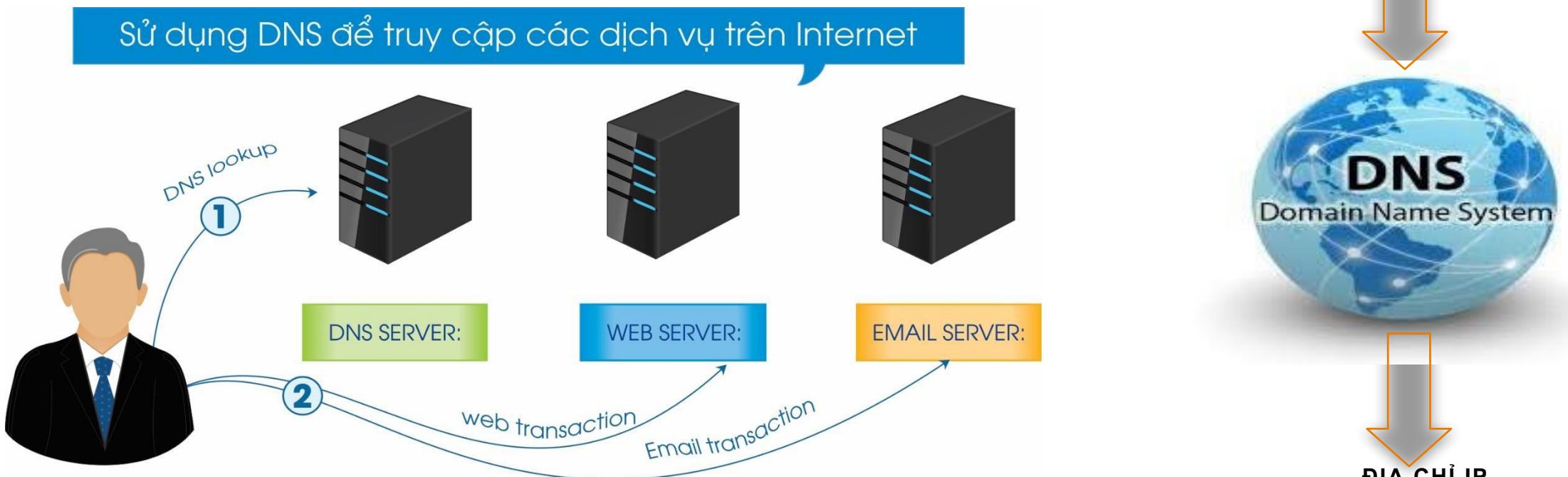
## ➤ 1.4. Xác thực thư điện tử Email Authentication

- ✓ Hệ thống thư điện tử (Email)
- ✓ Các mối đe dọa trong giao thư điện tử
- ✓ Email Authentication
- ✓ Giải pháp SPF
- ✓ Giải pháp DKIM
- ✓ Giải pháp DMARC

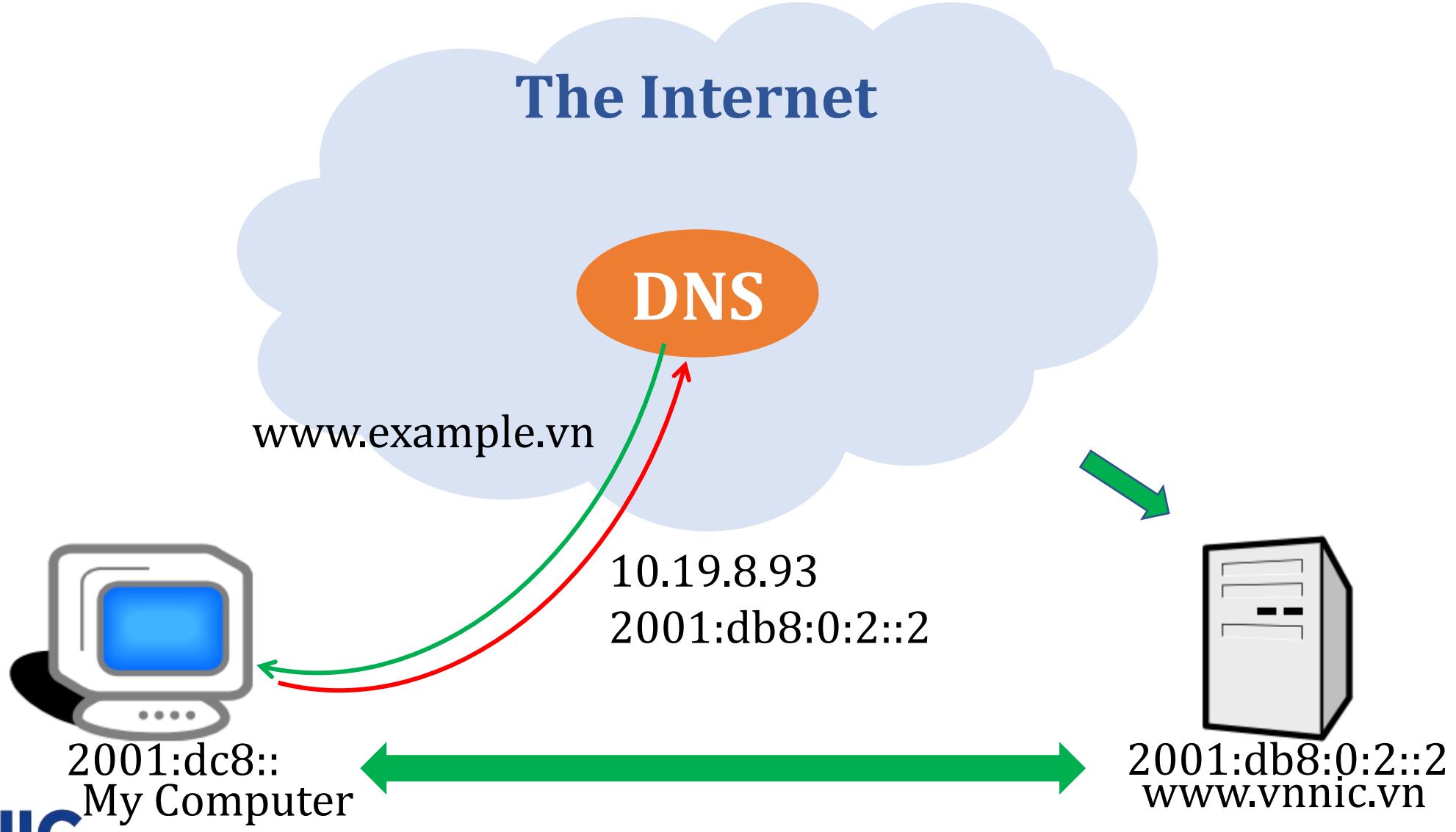
## HỆ THỐNG DNS LÀ GÌ?

# Hệ thống DNS là gì?

- ❖ **DNS (Domain Name Server):** Hệ thống tên miền



# Hệ thống DNS là gì?



# Hệ thống DNS là gì?

- ❖ Hệ thống phân giải tên miền sang địa chỉ IP:

**www.example.vn** → **10.10.30.3**

**academy.vnnic.vn** → **203.119.8.110**



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

**3.30.10.10.in-addr.arpa**

→ **www.example.vn**

**b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.8.e.2.0.c.6.7.0.1.0.0.2.ip6.arpa**

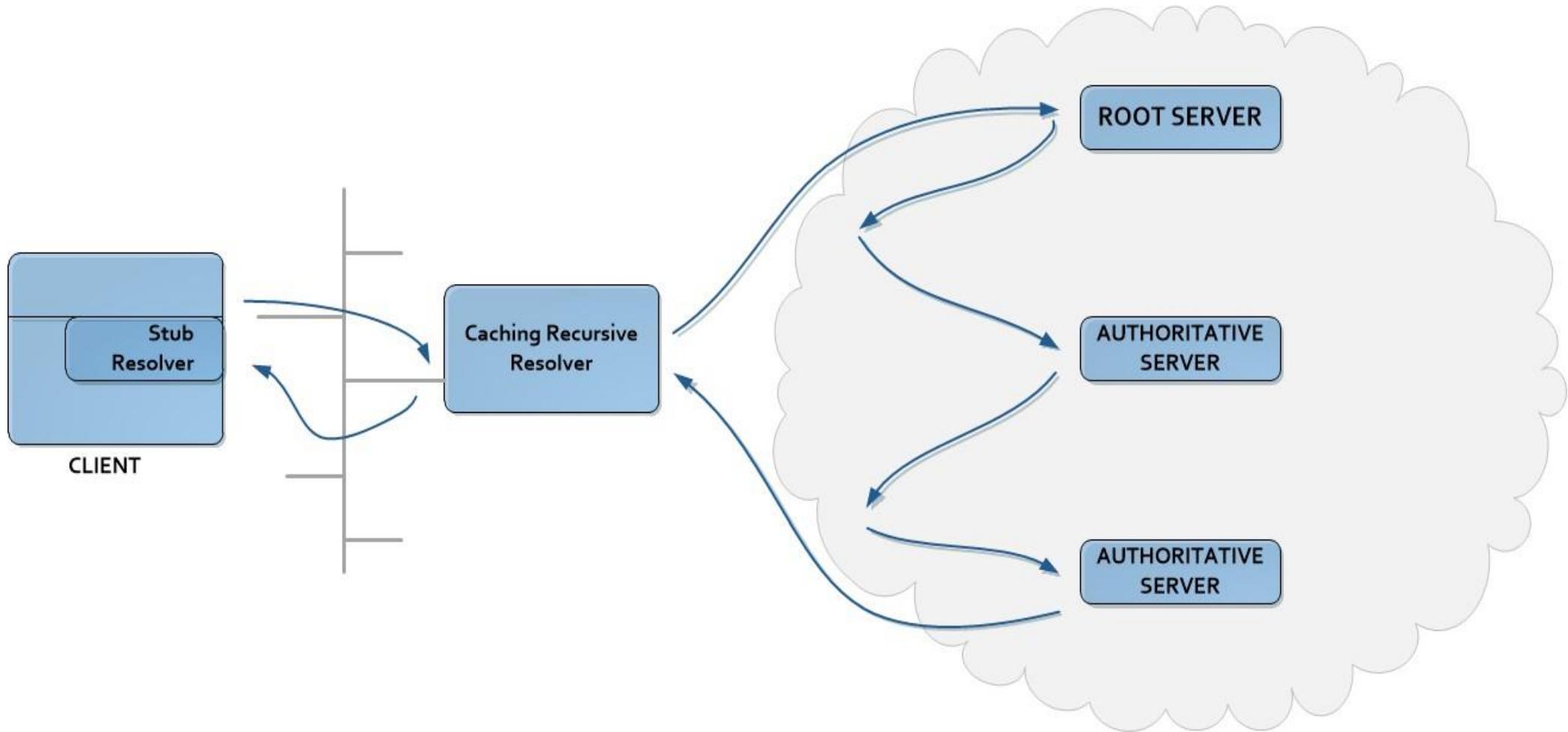
→ **academy.vnnic.vn**

## CÁC LOẠI MÁY CHỦ DNS

# Các loại máy chủ DNS

- **DNS Root**
- **DNS Authoritative**
- **DNS Cache**
- **DNS Forwarder**
- **DNS Hybrid**

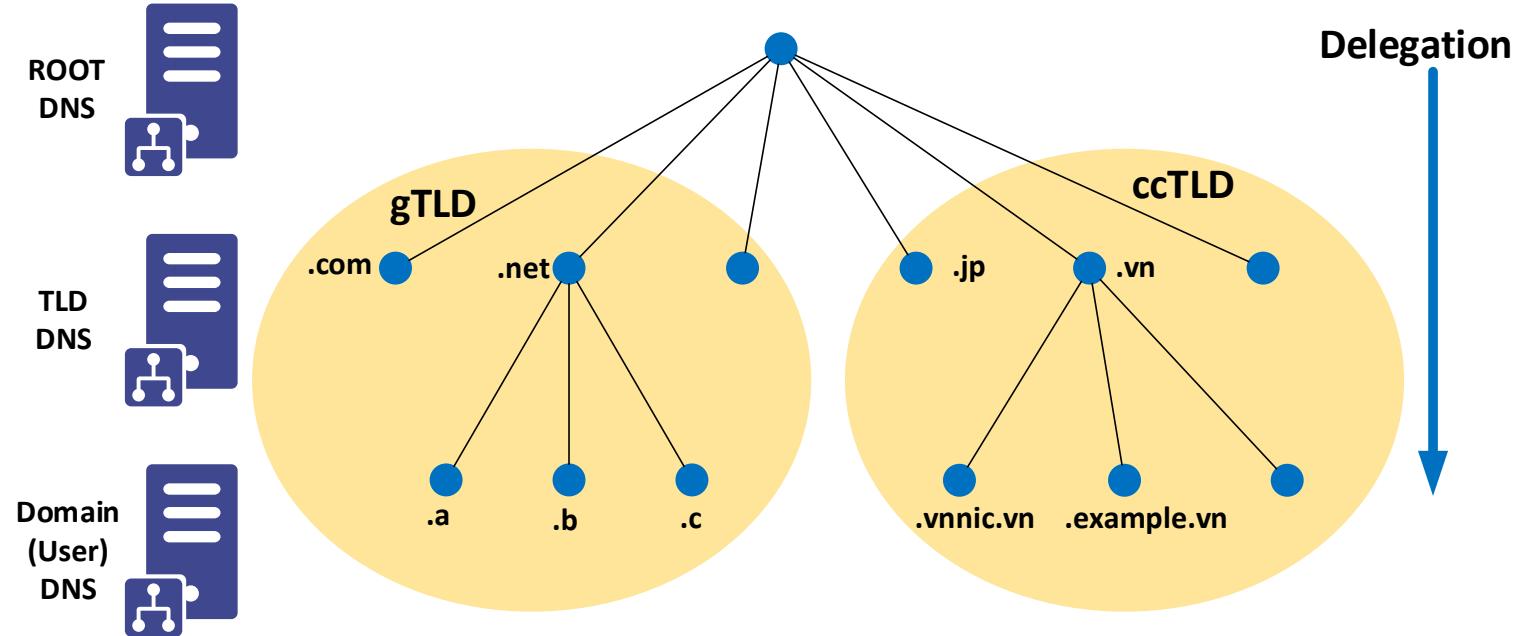
# Các loại máy chủ DNS



# Các loại máy chủ DNS

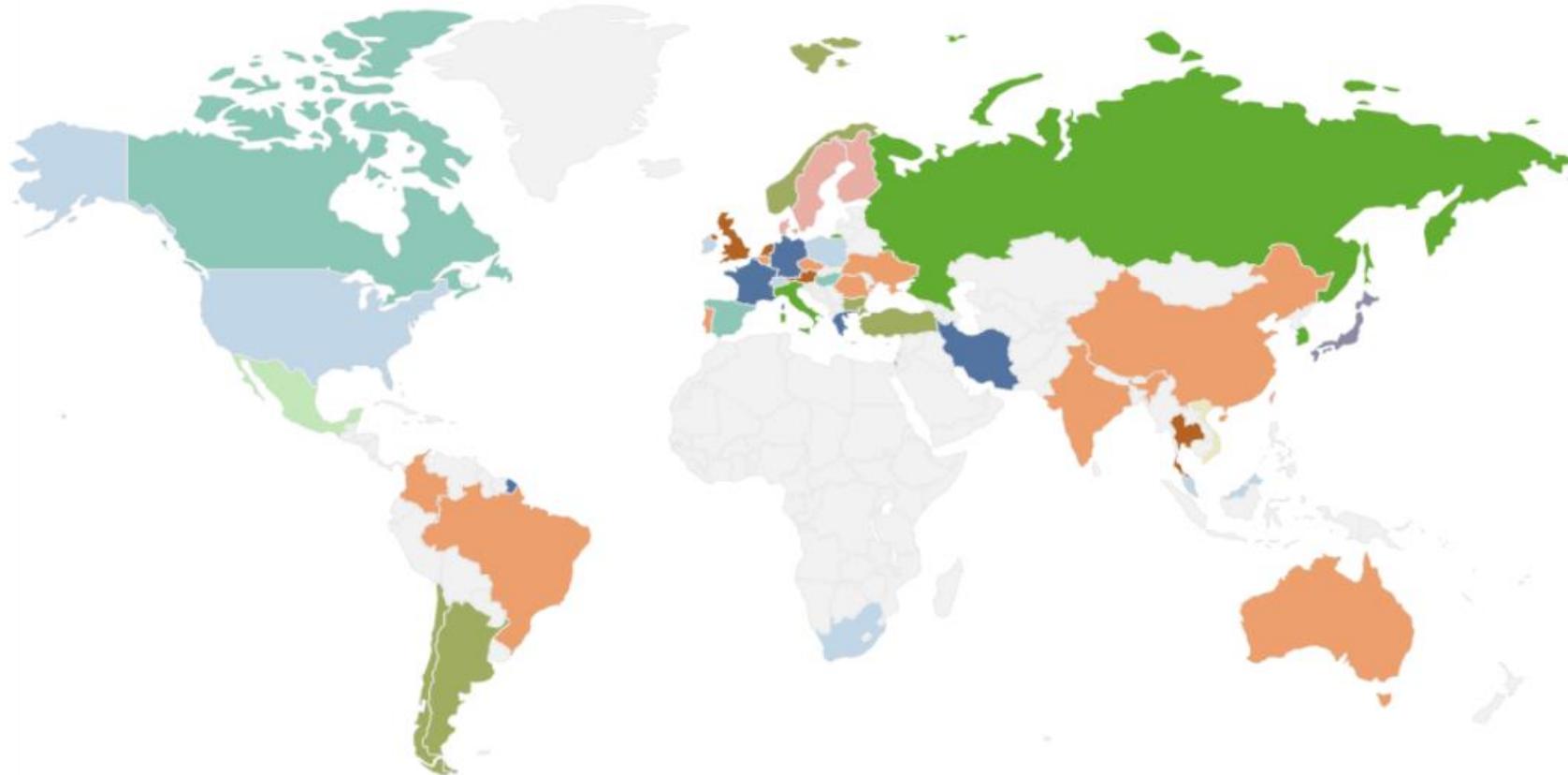
## ❖ Tổ chức máy chủ DNS

- Hệ thống máy chủ DNS xây dựng theo cơ chế phân cấp, chuyển giao của tên miền.
- ROOT DNS, TLD DNS, Owner DNS ...



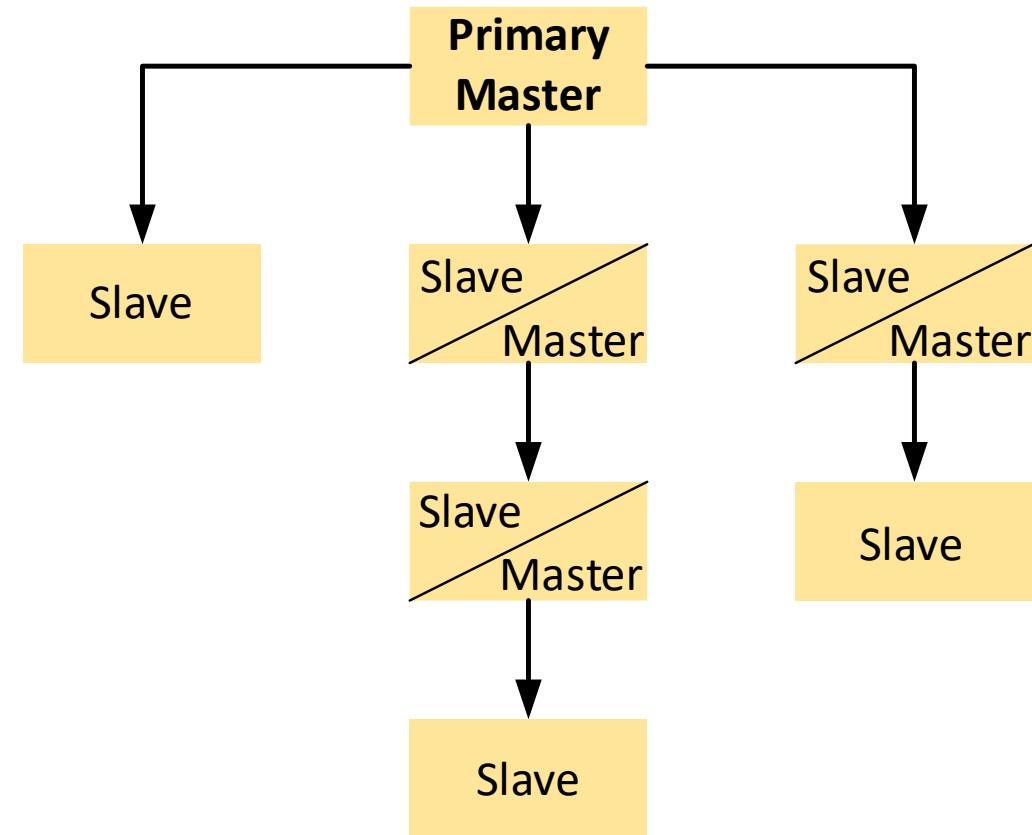
# Máy chủ DNS Root

- ❖ Máy chủ quản lý zone ":"
- ❖ 13 cụm máy chủ Root (<http://www.root-servers.org/>)



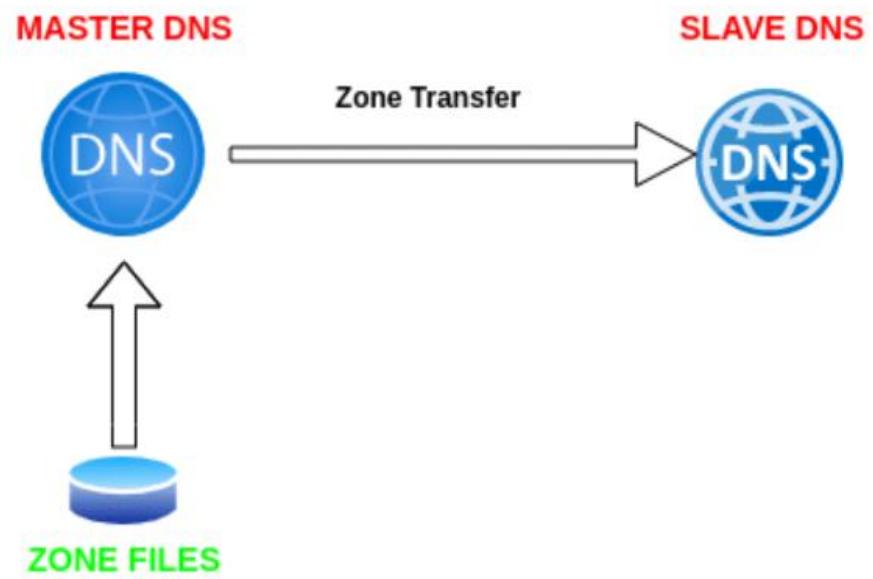
# Máy chủ DNS Authoritative

- ❖ Là các máy chủ DNS quản lý tên miền được chuyển giao (delegation).
- ❖ Quản lý toàn bộ bản ghi dữ liệu tên miền (RR) được chuyển giao.
- ❖ Trả lời truy vấn tên miền được phân cấp quản lý.
- ❖ Bao gồm máy chủ
  - Máy chủ DNS Primary/Master
  - Máy chủ DNS Secondary/Slave



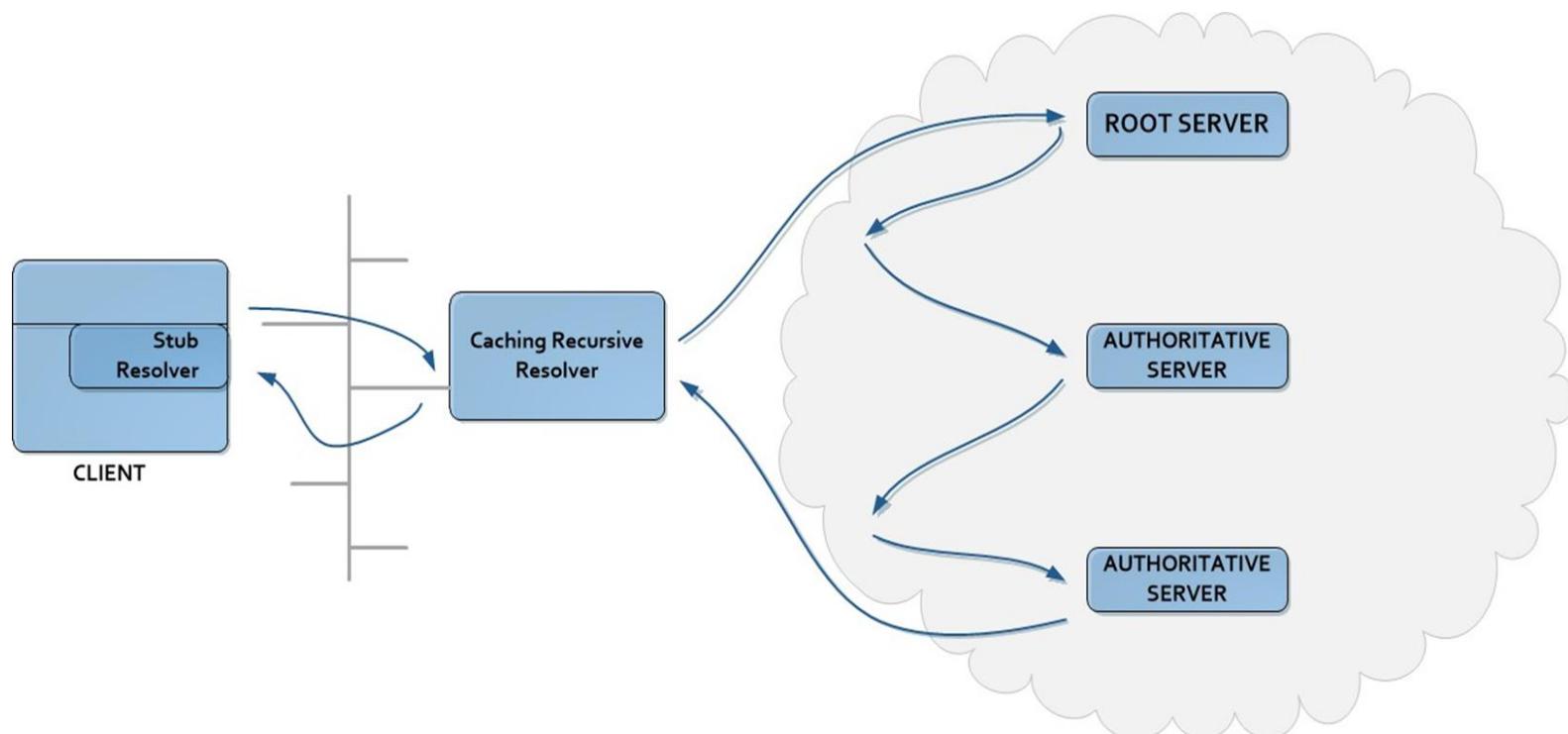
# Máy chủ DNS Authoritative

- ❖ Quá trình đồng bộ gọi là Zone Transfer
- ❖ Đồng bộ dữ liệu bản ghi tên miền từ máy chủ DNS Primary/Master sang máy chủ DNS Secondary/Slave.
  - Khi có thông báo (notify) từ máy chủ DNS Primary/Master.
  - Đồng bộ theo thời gian định kỳ.
  - Đồng bộ khi khởi động dịch vụ.
- ❖ Một tên miền chỉ có 01 máy chủ DNS Primary/Master và nhiều máy chủ DNS Secondary/Slave.



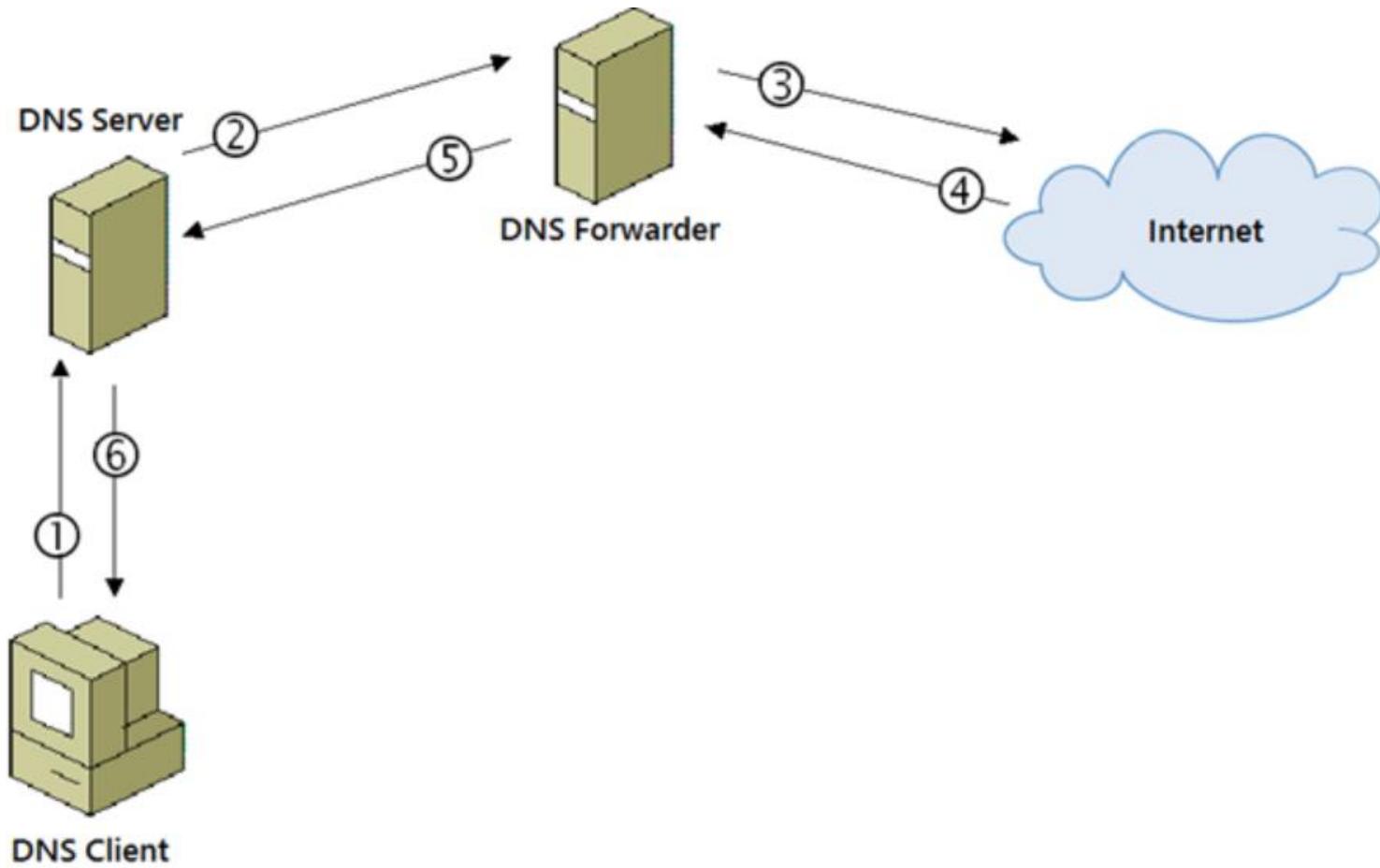
# Máy chủ DNS Cache

- ❖ Máy chủ không được chuyển giao tên miền.
- ❖ Thực hiện truy vấn đệ quy tìm ra câu trả lời cuối cùng cho người dùng.
- ❖ Lưu giữ dữ liệu truy vấn được tạm thời trong bộ nhớ để trả lời cho các truy vấn tiếp theo.



# Máy chủ DNS Forwarder

- ❖ Máy chủ tiếp nhận và chuyển tiếp truy vấn tên miền đến một máy chủ DNS chủ đích.



- ❖ Máy chủ DNS kết hợp 2 hoặc nhiều loại máy chủ:

- DNS Authoritative + DNS Cache
- DNS Cache + DNS Forwarder
- DNS Authoritative + DNS Cache + DNS Forwarder
- ....

## FILE DỮ LIỆU VÀ BẢN GHI TÊN MIỀN

# File dữ liệu và bản ghi tên miền

- ❖ **File dữ liệu**
- ❖ **Bản ghi tên miền**
  - ✓ **Cấu trúc bản ghi**
  - ✓ **Các loại bản ghi: SOA, NS, A, AAAA, CNAME, MX, PTR, ...**

# File dữ liệu và bản ghi tên miền

## ❖ File dữ liệu:

- Là nơi lưu trữ thông tin khai báo **các bản ghi tên miền**, các bản ghi ánh xạ (thuận/ngược) tên miền vào dịch vụ tương ứng.
- Có nhiều kiểu bản ghi khác nhau (RFC 1035).
  - ✓ Bản ghi SOA xác định các thông số quản lý tên miền, cung cấp thông tin về người quản trị, e-mail, các thông tin về thời gian cập nhật, lưu giữ dữ liệu ...
  - ✓ Bản ghi NS liệt kê các máy chủ quản lý tên miền cung cấp thông tin về máy chủ DNS lưu giữ thông tin về Zone.
  - ✓ Các bản ghi khác (A, AAAA, PTR, CNAME, TXT, WKS, HINFO) liệt kê các dữ liệu liên quan đến tên miền.

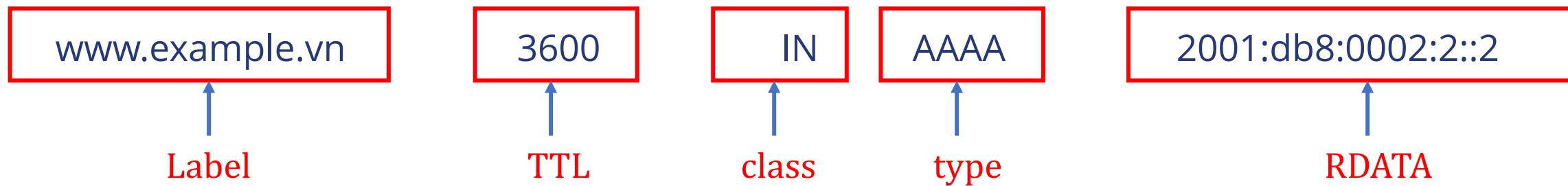
# File dữ liệu và bản ghi tên miền

## ❖ Bản ghi tên miền

### ➤ Cấu trúc bản ghi tên miền

Các bản ghi tên miền gồm:

- ✓ Tên (label)
- ✓ TTL (Time To Live): Thông số thời gian tồn tại của bản ghi tên miền
- ✓ Class: Không gian sử dụng tên miền
- ✓ Type: Các kiểu bản ghi tên miền
- ✓ Rdata: Dữ liệu ánh xạ với tên miền



# Các loại bản ghi tên miền

- ❖ Bản ghi tên miền: **Resource Record (RR)**
  - SOA: Start of Authority
  - NS: Name Server
  - A: bản ghi địa chỉ IPv4
  - AAAA: bản ghi địa chỉ IPv6
  - CNAME: bản ghi bí danh (Canonical Name - Alias)
  - MX: Mail Exchanger
  - PTR: Point Record (truy vấn ngược)
  - Các loại bản ghi khác: DKIM, DNSKEY, NSEC, ...

\$TTL 1d	Default TTL of 1 day
\$ORIGIN example.com.	Default FQDN to attach
@ IN SOA ns1.example.com. admin.example.com. (2013091200 ; se = serial number 12h ; ref = refresh 15m ; ret = refresh retry 3w ; ex = expiry 2h ; nx = nxdomain ttl )	SOA (Start of Authority)
IN NS ns1.example.com. IN NS ns2.example.net.	NS record
3w IN MX 10 mail.example.com. IN MX 20 mail.example.net.	MX record
ns1 IN A 172.16.140.41 mail IN A 172.16.140.42 joe IN A 172.16.140.43 www IN A 172.16.140.44	A record
ftp IN CNAME ftp.example.net.	CNAME record

# Các loại bản ghi tên miền

## ❖ **Bản ghi SOA (Start Of Authority)**

- Là bản ghi được khai báo đầu tiên trong file dữ liệu.
- Bản ghi SOA chỉ ra máy chủ tên miền này chính là nơi lưu giữ dữ liệu cho tất cả các tên miền thuộc tên miền được khai báo trong file này.
- Mỗi file dữ liệu chỉ có một bản ghi SOA duy nhất.

```
; Start of authority record for atrust.com
atrust.com.    IN  SOA   ns1.atrust.com. hostmaster.atrust.com. (
                           2009070200 ; Serial number
                           10800      ; Refresh      (3 hours)
                           1200       ; Retry        (20 minutes)
                           3600000   ; Expire       (40+ days)
                           3600 )     ; Minimum     (1 hour)
```

# Các loại bản ghi tên miền

## ❖ Bản ghi SOA (Start Of Authority)

2009070200	; Serial number
10800	; Refresh (3 hours)
1200	; Retry (20 minutes)
3600000	; Expire (40+ days)
3600 )	; Minimum (1 hour)

- Serial Number: Tham số phục vụ đồng bộ dữ liệu zone giữa các máy chủ DNS Primary/Master và Secondary/Slave.
- Refresh: Khoảng thời gian định kỳ DNS Secondary/Slave kết nối tới DNS Primary/Slave để thực hiện đồng bộ dữ liệu.
- Retry: Thời gian thực hiện lại sau lần refresh time từ DNS Secondary đến DNS Primary không thành công
- Expire: Khoảng thời gian DNS Secondary dữ liệu của zone không còn hiệu lực nếu không kết nối đến được DNS Primary
- Minimum TTL: Thời gian lưu trữ dữ liệu trên DNS Cache đối với các bản ghi không tồn tại.

# Các loại bản ghi tên miền

## ❖ Bản ghi SOA (Start Of Authority)

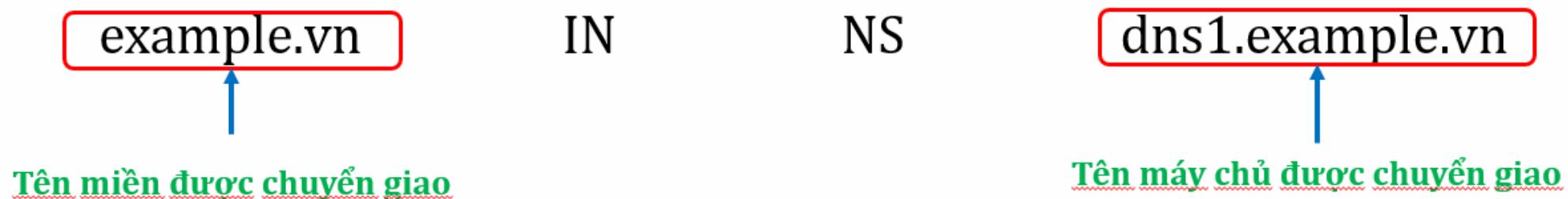
\$TTL 7200

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.

# Các loại bản ghi tên miền

## ❖ **Bản ghi NS (Name Server)**

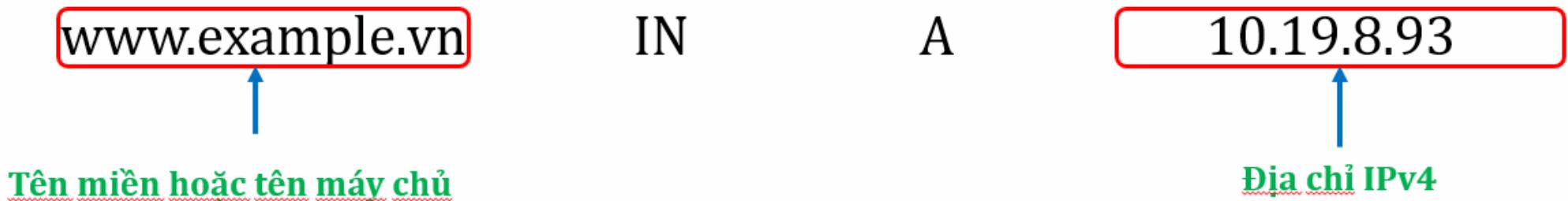
- Là bản ghi khai báo chuyển giao quản lý zone tên miền cho các máy chủ quản lý
- Bản ghi được khai báo trên cả trong zone cha và zone con.
- rdata là tên của máy chủ được chuyển giao DNS
- Tối thiểu 2 máy chủ chuyển giao tương ứng với 2 bản ghi NS để đảm bảo tính dự phòng.



# Các loại bản ghi tên miền

## ❖ Bản ghi A (Addresss)

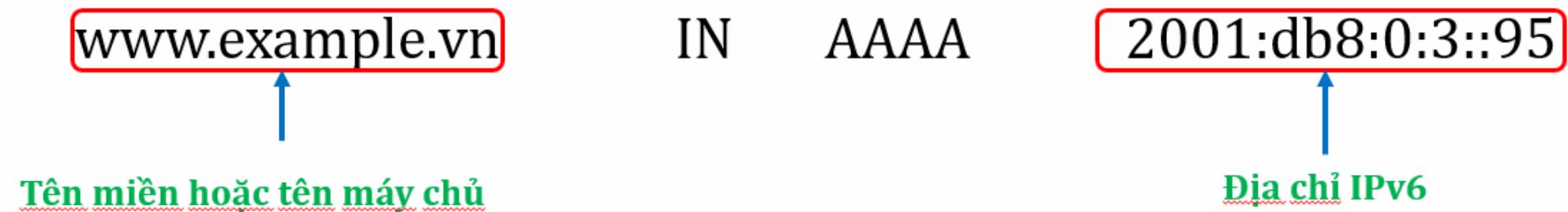
- Là bản ghi khai báo địa chỉ IPv4
- Rdata là địa chỉ IPv4



# Các loại bản ghi tên miền

## ❖ Bản ghi AAAA

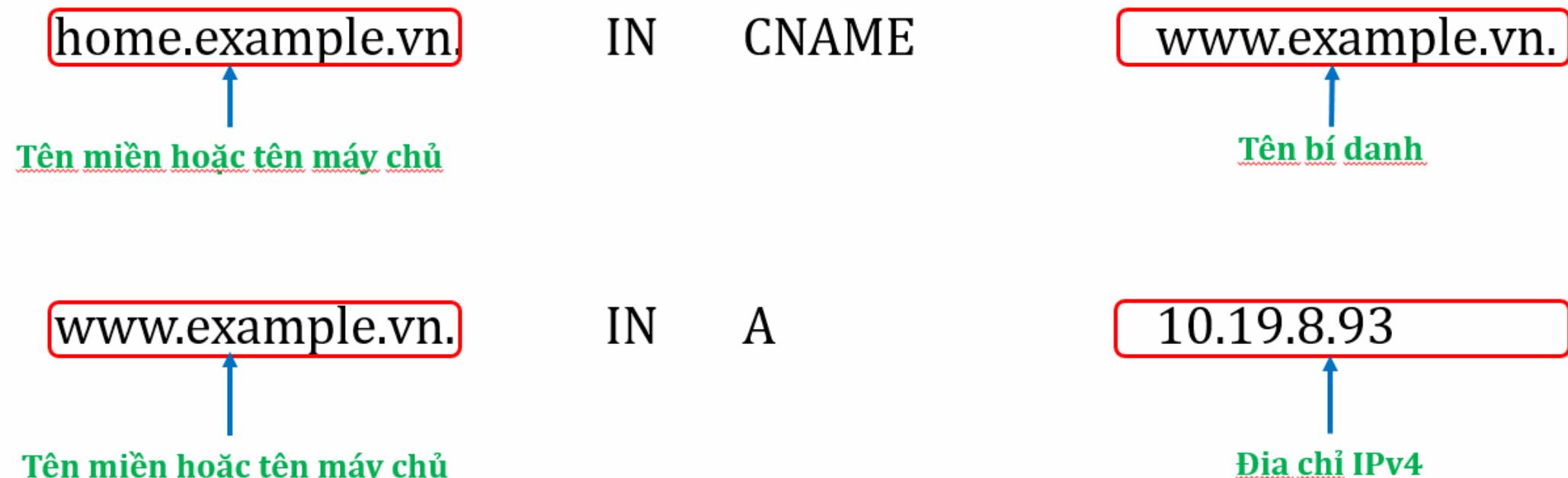
- Là bản ghi khai báo địa chỉ IPv6
- Rdata là địa chỉ IPv6



# Các loại bản ghi tên miền

## ❖ **Bản ghi CNAME (Canonical Name Record):** Bản ghi bí danh

- Sử dụng với trường hợp khai báo nhiều tên miền có cùng 01 địa chỉ IP.
- Bản ghi CNAME được khai báo cùng với bản ghi A hoặc AAAA
- Rdata là tên miền bí danh



## ❖ **Bản ghi MX (Mail Exchanger Record)**

- Là bản ghi sử dụng để khai báo trạm chuyển tiếp thư điện tử của một tên miền.
- rdata bao gồm tham số ưu tiên và địa chỉ của thư điện tử.
- Cấu trúc như sau:

Domainname	TTL	IN	MX	prefer	domainname
------------	-----	----	----	--------	------------

- Ví dụ:

example.vn	IN	MX	10	mail1.example.vn.
------------	----	----	----	-------------------

example.vn	IN	MX	20	mail2.example.vn.
------------	----	----	----	-------------------

# Các loại bản ghi tên miền

## ❖ **Bản ghi PTR (Point Record):** bản ghi ngược:

- Là bản ghi cho phép khai báo chuyển đổi địa chỉ IPv4/IPv6 sang tên miền.
- Ví dụ:

12.0.162.203.in-addr.arpa. IN PTR home.example.vn.

Địa chỉ IPv4 tên miền ngược

Tên miền hoặc hostname

5.1.1.0.5.0.0.0.8.c.d.0.1.0.0.2.ipv6.arpa.

Địa chỉ IPv6 tên miền ngược

IN PTR ipv6.example.vn.

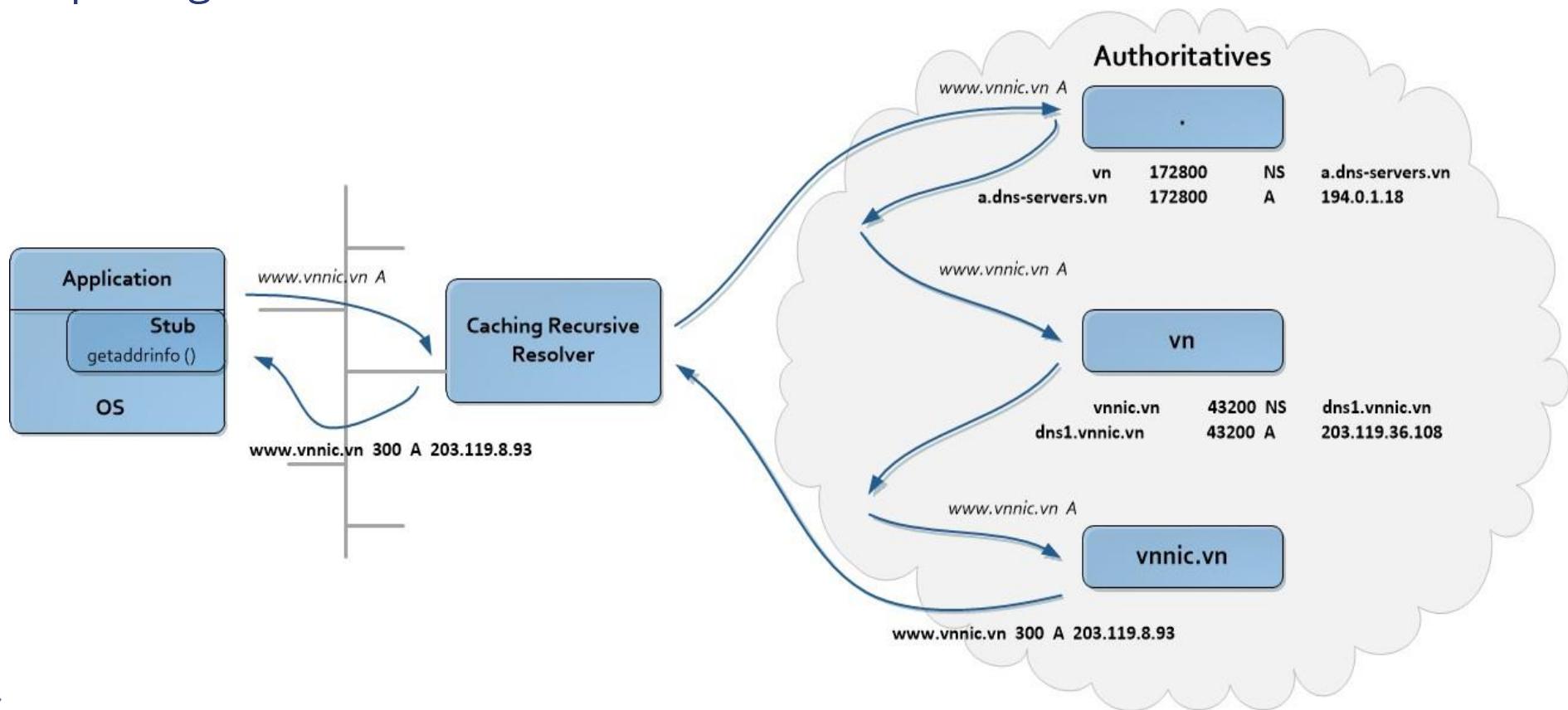
Tên miền hoặc hostname

# PHẦN 1: HỆ THỐNG DNS

## HOẠT ĐỘNG CỦA HỆ THỐNG DNS

# Hoạt động của hệ thống DNS

- ❖ Chuyển giao zone tên miền
- ❖ Phân giải tên miền
- Quá trình phân giải tên miền **vnnic.vn.**



# PHẦN 1: HỆ THỐNG DNS

## CÀI ĐẶT VÀ CẤU HÌNH HỆ THỐNG DNS

# Cài đặt và cấu hình hệ thống DNS

## ❖ Cài đặt hệ thống DNS

- ✓ Phần mềm DNS
- ✓ Chuẩn bị
- ✓ Cài đặt
- ✓ Giải nén
- ✓ Kiểm tra

## ❖ Cấu hình hệ thống DNS

- ✓ Phần mềm DNS
- ✓ File cấu hình
- ✓ File dữ liệu
- ✓ Cấu hình Master – Slave
- ✓ Cấu hình hoạt động DNS Cache

# Cài đặt và cấu hình hệ thống DNS

## ❖ Phần mềm DNS

- Có nhiều phần mềm DNS khác nhau: BIND, Windows DNS, CNS/ANS, NSD/Unbound, Knot, PowerDNS,...
- Phần mềm BIND là phần mềm phổ biến nhất:
  - ✓ Mã nguồn mở, miễn phí
  - ✓ Hỗ trợ Windows, Linux, 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 ...

# Cài đặt và cấu hình hệ thống DNS

## ❖ Chuẩn bị

➤ Tải phần mềm BIND

- ✓ Truy cập <http://www.isc.org>
- ✓ Vào phần Download → BIND và tải về gói tar.gz mới nhất.
- ✓ Sử dụng các chương trình SFTP (trong SSH), FTP để đưa gói lên máy chủ.

➤ Cài đặt một số công cụ, thư viện hỗ trợ cài đặt phần mềm BIND:

- ✓ gunzip, tar, gcc, make,...

# Cài đặt và cấu hình hệ thống DNS

## ❖ 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 viết thêm 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 và cấu hình hệ thống DNS

## ❖ Cài đặt

- Để cài đặt sử dụng các thiết lập mặc định, chúng ta thực hiện tuần tự các lệnh sau để cài BIND
  - ✓ # ./configure
  - ✓ # make all
  - ✓ # make install
- Mặc định các file chương trình của bind sẽ được cài tại thư mục:
  - ✓ /usr/local/sbin và /usr/local/bin

# Cài đặt và cấu hình hệ thống DNS

## ❖ Kiểm tra

- Để kiểm tra BIND phiên bản phần mềm BIND, dùng lệnh: /usr/local/sbin/named -v
  - ✓ # named -v
  - ✓ BIND 9.11.17-P1
- Xem các file cài đặt
  - ✓ ls /usr/local/sbin
    - dnssec-keygen, dnssec-makekeyset, dnssec-signkey, dnssec-signzone
    - lwresd, named-checkconf, named-checkzone
    - rndc, rndc-confgen
    - named
  - ✓ ls /usr/local/bin
    - dig
    - host, isc-config.sh, nslookup
    - nsupdate

# Cài đặt và cấu hình hệ thống DNS

- ❖ BIND hoạt động cần có file cấu hình & 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 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 files)
  - Kiểm tra cấu trúc của file cấu hình & file dữ liệu
  - Chạy chương trình DNS (named)

# Cài đặt và cấu hình hệ thống DNS

## ❖ File cấu hình

- **acl**: Defines a named IP address matching list for access control and other uses.
- **control**: Defines the control channels used by the rndc utility.
- **include**: Includes a file.
- **key**: Specifies key information for use in authentication and authorization using TSIG.
- **logging**: Specifies what the server logs and where the log messages are stored.
- **options**: Controls global server configuration options and sets defaults for other statements.
- **server**: Sets certain configuration options on a per server basis.
- **trusted-keys**: Defines trusted DNSsec keys.
- **view**: Defines a view. (This statement is used from version 9 onwards.)
- **zone**: Defines a zone

# Cài đặt và cấu hình hệ thống DNS

## ❖ 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;
};
```

# Cài đặt và cấu hình hệ thống DNS

## ❖ Hướng dẫn kiểm tra file cấu hình

- Để 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 gì và ở đâu.
- Dựa trên thông báo, điều chỉnh lại cấu hình cho phù hợp.
- Sau khi sửa xong và lưu lại các thông số được sửa, chúng ta phải thực hiện lại lệnh kiểm tra file cấu hình và file dữ liệu để đảm bảo cú pháp và nội dung file đã đúng.

# Cài đặt và cấu hình hệ thống DNS

## ❖ File dữ liệu:

- Lưu trữ các bản ghi tài tên miền của tên miền (zone) mà máy chủ DNS đó quản lý
- 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
```

# Cài đặt và cấu hình hệ thống DNS

## ❖ Kiểm tra file dữ liệu:

- Kiểm tra file dữ liệu sử dụng câu lệnh:
  - ✓ named-checkzone "zonename" "filename"
- Trong trường hợp file dữ liệu có lỗi cú pháp, chương trình sẽ thông báo lỗi gấp 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, người quản trị nên 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

# Cài đặt và cấu hình hệ thống DNS

## ❖ Chạy dịch vụ DNS

- File chương trình máy chủ DNS của BIND là named (/usr/local/sbin/named)
- Chạy chương trình với file cấu hình:
  - ✓ `#/usr/local/sbin/named -c /etc/named.conf`
- Thông tin khi chạy mặc định sẽ đưa vào syslog của hệ thống
  - ✓ `/var/log/message.`
  - ✓ Xem log: `tail -f /var/log/message`
- Thông thường: mở 02 cửa sổ xem log và chạy named đồng thời để quan sát thời gian thực.

# Cài đặt và cấu hình hệ thống DNS

## ❖ Chạy dịch vụ DNS

➤ Kiểm tra tiến trình PID 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.

➤ Khởi động lại:

✓ #kill -HUP PID

➤ Tắt chương trình:

✓ #kill -9 PID

# Cài đặt và cấu hình hệ thống DNS

## ❖ Cấu hình hoạt động Master/Slave:

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

# Cài đặt và cấu hình hệ thống DNS

## ❖ Cấu hình hoạt động DNS Cache:

- Không quản lý tên miền nào.
- Thực hiện truy cẩn recursive
- Sử dụng “hint zone”.

```
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;
};
```

# PHẦN 1: HỆ THỐNG DNS

## QUẢN TRỊ VÀ GỠ LỖI DNS

# Quản trị và gỡ lỗi DNS

- ❖ Kiểm tra dịch vụ DNS
- ❖ Bật/tắt dịch vụ DNS
- ❖ RNDC
- ❖ NSLOOKUP, DIG
- ❖ Nhật ký hoạt động (Log)

## ❖ Kiểm tra dịch vụ DNS

- Để kiểm tra máy chủ tên miền đã hoạt động chưa, ta dùng lệnh
  - ✓ #ps -ef | grep named
- Nếu chương trình named đã hoạt động, chúng ta có thể thấy được Process ID của chương trình và sẽ nhận được thông báo giống như sau:
  - ✓ #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 là 12640
- Kiểm tra file cấu hình, file dữ liệu:
  - ✓ File cấu hình: named-checkconf
  - ✓ File dữ liệu: named-checkzone

## ❖ Bật/tắt 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 do đó để chạy chương trình named chúng ta dùng lệnh sau:
  - ✓ # /usr/local/sbin/named -c /etc/named.conf
- Để tắt dịch vụ DNS dùng lệnh sau:
  - ✓ Kill -9 PID (Process ID)
- Để restart dịch vụ DNS dùng lệnh sau:
  - ✓ Kill -HUP PID

## ❖ RNDC

- rndc (remote name server control) là công cụ cho phép điều khiển BIND từ xa, đảm bảo an toàn
- 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

# Quản trị và gỡ lỗi DNS

## ❖ RNDC

### 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";};  
};
```

# Quản trị và gỡ lỗi DNS

## ❖ RNDC

Command	Description
reload	Reloads the configuration file and zone files
reconfig	Reloads the configuration file and new or changed zone files; unchanged zone files are not loaded
stats	Records the statistics into a file
querylog	Switches on logging queries about the name server
dumpdb	Records the server's cache memory in the dump file
stop	Stops the server and records changes acquired by IXFR or by a dynamic update into files
halt	Stops the server immediately
trace	Increases the debugging level of the server by 1
notrace	Sets the debugging level of the server at 0
flush	Cleans the server's cache memory
status	Displays the status of the server

## ❖ NSLOOKUP

- Là một tiện ích tra cứu tên miền trên hệ thống DNS .
- Có sẵn trong Windows và UNIX.
- Thủ tục tra cứu khác với resolver tích hợp sẵn trong OS, sử dụng thư viện của resolver.
- Nslookup tương tác từng server <> resolver tương tác nhiều server.
- Có khả năng thực hiện zone transfer: nhưng không check SOA RR như slave DNS.
- Chỉ sử dụng DNS, không hỗ trợ NetBIOS names, LMHOSTS, or WINS
- Hoạt động interactively hoặc noninteractively

# Quản trị và gõ lỗi DNS

## ❖ NSLOOKUP

```
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 (Domain Information Groper)

- 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

# Quản trị và gỡ lỗi DNS

## ❖ DIG

- 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](http://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
```

# Quản trị và gỡ lỗi DNS

## ❖ DIG

- 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](http://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

### ➤ 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)

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

# Quản trị và gỡ lỗi DNS

## ❖ Nhật ký hoạt động (Log)

- **default:** 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
- **Iame-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 (request)
- **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

# Quản trị và gỡ lỗi DNS

## ❖ Nhật ký hoạt động (Log)

### ➤ 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;};
}
```

# PHẦN 1: HỆ THỐNG DNS

## AN TOÀN VÀ TỐI ƯU HỆ THỐNG DNS

# AN TOÀN VÀ TỐI ƯU HỆ THỐNG DNS

- ❖ **Tối ưu file cấu hình**
- ❖ **Tối ưu dịch vụ DNS Cache**
- ❖ **Tối ưu Zone Transfer**
- ❖ **Cân bằng tải dịch vụ**
- ❖ **Triển khai DNS Master-Slave**

## ❖ Tối ưu file cấu hình

- Cấu hình địa chỉ dịch vụ
  - ✓ version
  - ✓ Listen-on/ listen-on-v6;
- Cấu hình các tham số
  - ✓ source-query,
  - ✓ source-transfer
  - ✓ notify-on
  - ✓ allow-transfer, allow-query
- Cấu hình log
  - ✓ Phân tách các loại log thành các file dễ theo dõi
  - ✓ Quản lý vòng đời của file.
- Statistic
  - ✓ zone-statistics

## ❖ Tối ưu hoạt động DNS Cache

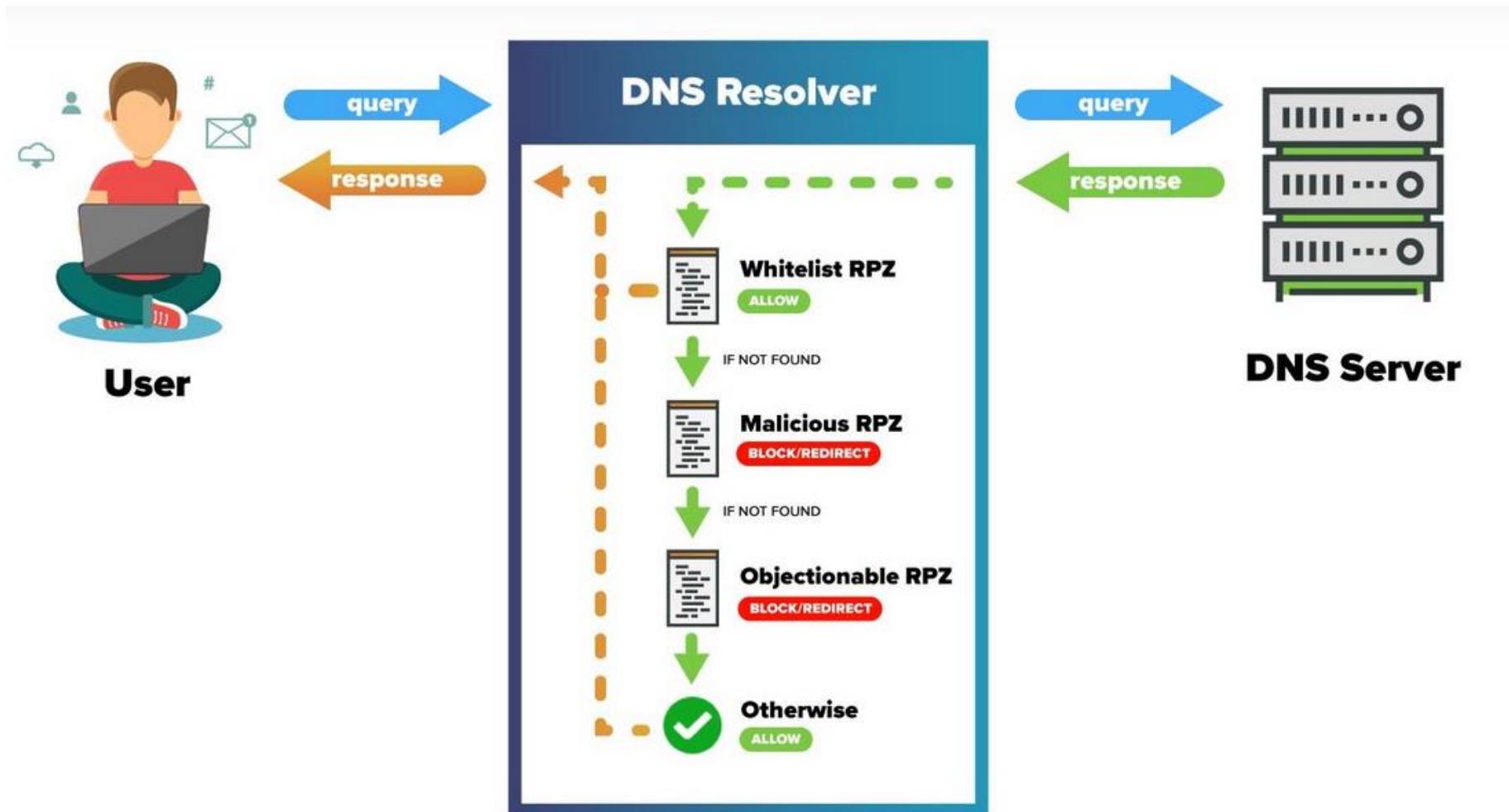
- Thiết lập thời gian negative-cache tối đa:
  - ✓ max-ncache-ttl
  - ✓ Mặc định: 3 giờ, max 7 ngày
  - ✓ Nếu thiết lập > 7 ngày, BIND đặt lại thành 7 ngày.
- Thiết lập thời gian cache tối đa
  - ✓ max-cache-ttl
  - ✓ Mặc định: 7 ngày.
- Thiết lập thời gian xóa bản ghi có TTL đã expire
  - ✓ cleaning-interval
  - ✓ Mặc định 60 phút.
- Thiết lập RPZ để đảm bảo an toàn

## Đảm bảo an toàn hoạt động DNS Cache sử dụng 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.

# AN TOÀN VÀ TỐI ƯU HỆ THỐNG DNS

## Đảm bảo an toàn hoạt động DNS Cache sử dụng RPZ



## Đảm bảo an toàn hoạt động DNS Cache sử dụng 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 Ransomware (phần mềm độc hại)
  - ✓ Chặn Botnet
  - ✓ Xác định máy chủ nhiễm mã độc hoặc bị Botnet.

## Đảm bảo an toàn hoạt động DNS Cache sử dụng RPZ

- ❖ RPZ được hỗ trợ trên một số phần mềm DNS phổ biến cho DNS Cache như:
  - BIND V9.9 (hoặc cao hơn)
  - Power DNS
- ❖ Một số DNS Cache đã thiết lập RPZ để hoạt động như:
  - Infloxblox
  - Efficient IP
  - BlueCat

## Đảm bảo an toàn hoạt động DNS Cache sử dụng RPZ

- ❖ 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
  - Sau khi đã tiến hành lọc theo 5 yếu tố, máy chủ DNS dựa trên các quy luật đã thiết lập 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.

## Đảm bảo an toàn hoạt động DNS Cache sử dụng RPZ

- ❖ 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; };
```

# AN TOÀN VÀ TỐI ƯU HỆ THỐNG DNS

## ❖ Ví dụ file zone RPZ

```
$TTL 2h;
$ORIGIN domain.example.com.
@           SOA nsd.example.net. hostmaster.example.com ( 1 12h 15m 3w 2h)
              NS nsd.example.net. // out-of-zone no A/AAAA RR required
; begin RPZ RR definitions

;; QNAME Trigger

; QNAME Trigger NXDOMAIN Action
; kills whole domain
example.org      CNAME .
*.example.org    CNAME .

; stops www.example.org etc.
; but would allow reading of MX/NS/SOA at apex
*.example.org    CNAME .

; QNAME Trigger NODATA Action
; kills whole domain
example.org      CNAME *.
*.example.org    CNAME *.

; QNAME Trigger PASSTHRU Action
; typically only used for bypass
mail.example.org CNAME rpz-passthru.

; QNAME Trigger DROP Action
; kills whole domain
example.org      CNAME rpz-drop.
*.example.org    CNAME rpz-drop.
```

## ❖ Tối ưu Zone Transfer

### ➤ SOA mẫu

example.vn. IN SOA dns1.example.vn.

hostmaster.example.vn. (

2009080800 ; serial number

12h ; refresh

15m ; update retry

3w ; expiry

1h ; minimum

)

### ➤ Tối ưu:

- ✓ Tổ chức Serial number hợp lý
- ✓ Thiết lập thời gian refresh
- ✓ Thiết lập thời gian update retry
- ✓ Thiết lập thời gian expire
- ✓ Thiết lập Negative TTL.

### ➤ Theo khuyến nghị RFC 1912

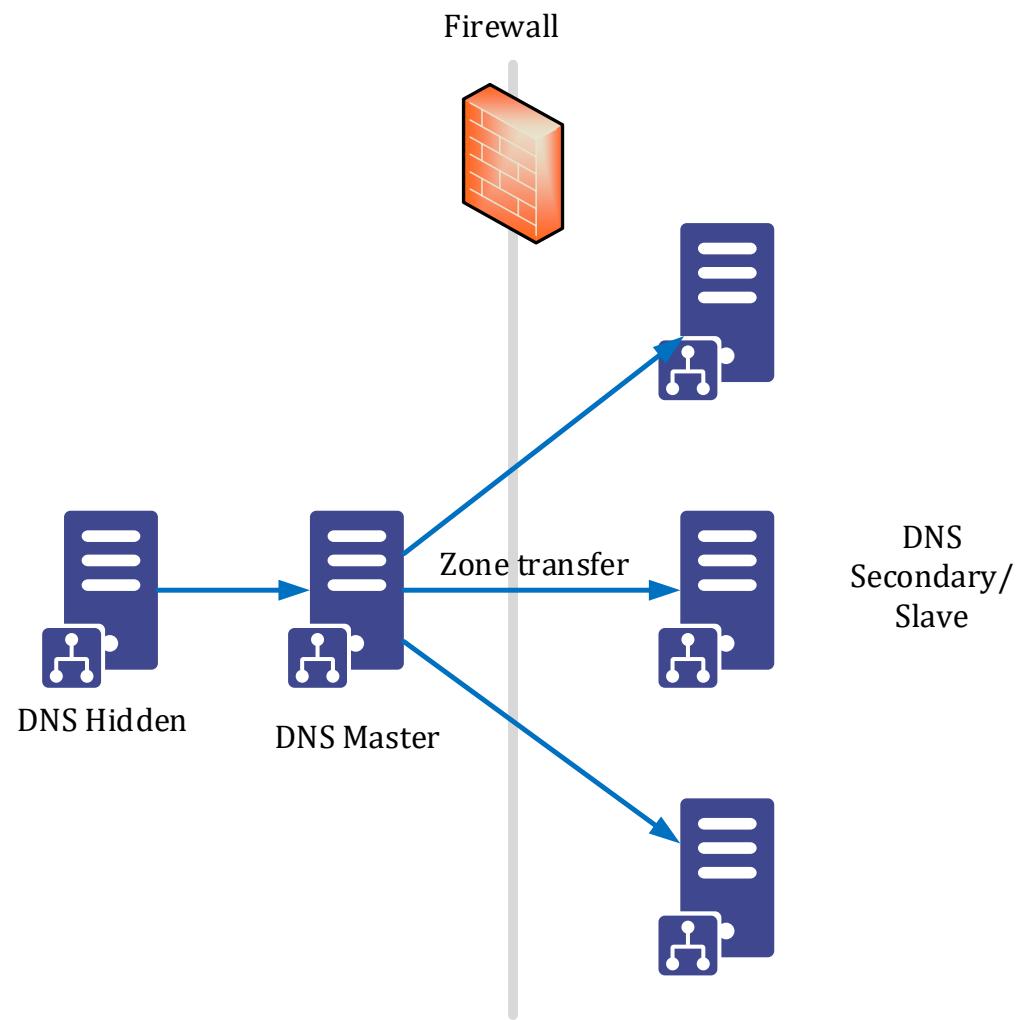
- ✓ Refresh time: 02 giờ → 12 giờ
- ✓ Retry time: 02 phút → 02 giờ
- ✓ Expire time: 02 → 04 tuần

## ❖ Cân bằng tải dịch vụ

- Sử dụng Slave DNS, tối đa 13 máy chủ.
- Triển khai tại nhiều vị trí khác nhau
  - ✓ Tăng tốc độ trả lời.
  - ✓ Tăng khả năng dự phòng.
- Đồng bộ dữ liệu qua AXFR hoặc IXFR
- Triển khai trên các OS và phần mềm khác nhau.
- Sử dụng cluster các máy chủ DNS.
- Sử dụng các cụm DNS Anycast.

## ❖ Triển khai DNS Master - Slave

- Master của cụm DNS
- Không phục vụ truy vấn từ bên ngoài.
- Đồng bộ dữ liệu qua AXFR hoặc IXFR



# PHẦN I: HỆ THỐNG DNS

## ➤ 1.1. Lý thuyết hệ thống DNS

- ✓ Hệ thống DNS là gì?
- ✓ Các loại máy chủ DNS
- ✓ File dữ liệu và bản ghi tên miền
- ✓ Hoạt động của hệ thống DNS
- ✓ Cài đặt và cấu hình hệ thống DNS
- ✓ Quản trị và gỡ lỗi DNS
- ✓ An toàn và tối ưu hệ thống DNS

## ➤ 1.2. DNS hoạt động IPv6

- ✓ Quá trình truy vấn, phân giải
- ✓ Khuyến nghị cho DNS hoạt động IPv6
- ✓ Hướng dẫn triển khai DNS hoạt động IPv6
- ✓ Chuyển đổi Website IPv6
- ✓ Khuyến nghị triển khai

## ➤ 1.3. DNSSEC

- ✓ Nguyên tắc an toàn an ninh hệ thống DNS
- ✓ Tấn công hệ thống DNS
- ✓ DNSSEC
- ✓ DNSSEC hoạt động như thế nào?
- ✓ Hoạt động truy vấn DNSSEC
- ✓ Các bản ghi tài nguyên mới
- ✓ Chain of Trust
- ✓ Triển khai DNSSEC trên hệ thống DNS Root

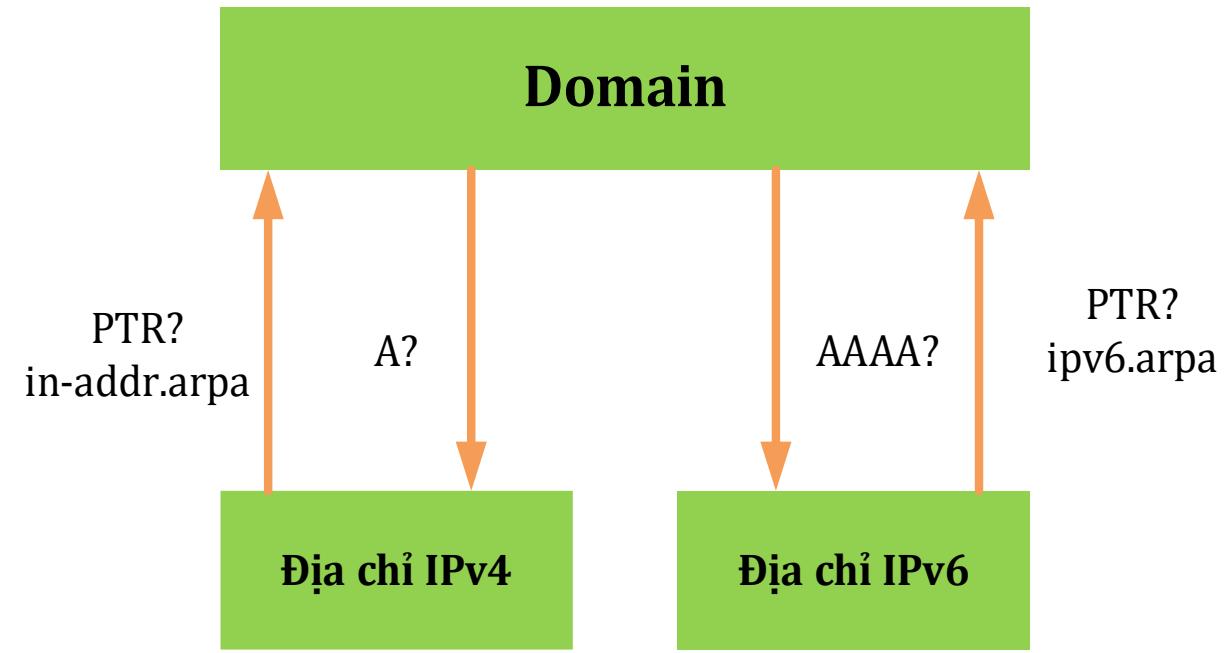
## ➤ 1.4. Xác thực thư điện tử Email Authentication

- ✓ Hệ thống thư điện tử (Email)
- ✓ Các mối đe dọa trong giao thư điện tử
- ✓ Email Authentication
- ✓ Giải pháp SPF
- ✓ Giải pháp DKIM
- ✓ Giải pháp DMARC

## DNS HOẠT ĐỘNG IPV6

# Quá trình truy vấn, phân giải

- ❖ 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 bit, điều này làm tăng tải xử lý và truyền dẫn trên mạng so với truy vấn địa chỉ IPv4.



# Quá trình truy vấn, phân giải

- ❖ 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

# 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 là:
  - RFC 3901: “DNS IPv6 Transport Operational Guidelines”
  - RFC4472: “Operational Considerations and Issues with IPv6”
- ❖ Hai 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

- ❖ 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 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

## ❖ Thiết lập qua tham số

```
➤ options { listen-on-v6 { IPv6_Servers; }; };  
➤ options { transfer-source-v6 IPv6_Servers; };  
➤ options { notify-source-v6 IPv6_Servers; };
```

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

## ❖ Thuê dịch vụ NCC

- 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://www.ipaddressguide.com/ipv6-check/>
    - Bước 2: Chọn mục Website trên thanh menu.
    - 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

- 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](mailto:IPv6ForGov@vnnic.vn).
  - ✓ Danh sách website hoạt động & được gán nhãn IPv6 Ready Logo sẽ công bố trên Website Vietnam IPv6 Ready.



The screenshot shows a web browser window with the URL [vietnamipv6ready.vn/website/danh sach](http://vietnamipv6ready.vn/website/danh sach). The page features a banner for 'VIET NAM IPv6 READY' with the Vietnamese flag and a large 'IPv6 READY' logo. Below the banner is a navigation menu with links: TRANG CHỦ | TÀI NGUYÊN | WEBSITE | DỊCH VỤ VÀ PHẦN MỀM | THIẾT BỊ | IPV6 USER | LIÊN KẾT | LIÊN HỆ. A table titled 'Danh sách website chạy IPv6' displays 101 entries. The table has three columns: 'Sites' (website URLs), 'Đơn vị chủ quản' (Managing body), and 'Đã gán nhãn IPv6 ready logo' (Has IPv6 ready logo assigned). Most sites listed have not yet been assigned a logo.

Sites	Đơn vị chủ quản	Đã gán nhãn IPv6 ready logo
<a href="https://bkns.vn">https://bkns.vn</a>	Công ty TNHH Giải pháp mạng Bạch Kim	Chưa gán nhãn
<a href="http://ict-hcm.gov.vn">http://ict-hcm.gov.vn</a>	Sở Thông tin và Truyền thông thành phố Hồ Chí Minh	Đã gán nhãn
<a href="http://www.hochiminhcity.gov.vn">http://www.hochiminhcity.gov.vn</a>	Ủy ban nhân dân thành phố Hồ Chí Minh	Đã gán nhãn
<a href="https://telecom.qpsc.com.vn">https://telecom.qpsc.com.vn</a>	Công ty TNHH MTV Phát triển Công viên phần mềm Quang Trung	Chưa gán nhãn
<a href="https://www.dongnai.gov.vn">https://www.dongnai.gov.vn</a>	Ủy ban nhân dân tỉnh Đồng Nai	Đã gán nhãn
<a href="https://www.qpsc.com.vn">https://www.qpsc.com.vn</a>	Công ty TNHH MTV Phát triển Công viên phần mềm Quang Trung	Đã gán nhãn
<a href="https://www.m3complex.vn">https://www.m3complex.vn</a>	Công ty TNHH MTV Thông tin M3	Chưa gán nhãn
<a href="http://alta.gov.vn">http://alta.gov.vn</a>	Cục Tin học hóa - Bộ Thông tin và Truyền thông	Đã gán nhãn
<a href="http://monre.gov.vn">http://monre.gov.vn</a>	Bộ Tài nguyên và Môi trường	Chưa gán nhãn
<a href="https://danang.gov.vn/">https://danang.gov.vn/</a>	Ủy ban nhân dân thành phố Đà Nẵng	Chưa gán nhãn
<a href="https://tttt.danang.gov.vn">https://tttt.danang.gov.vn</a>	Sở Thông tin và Truyền thông thành phố Đà Nẵng	Chưa gán nhãn
<a href="https://mail.lamdong.gov.vn">https://mail.lamdong.gov.vn</a>	Ủy ban nhân dân tỉnh Lâm Đồng	Đã gán nhãn

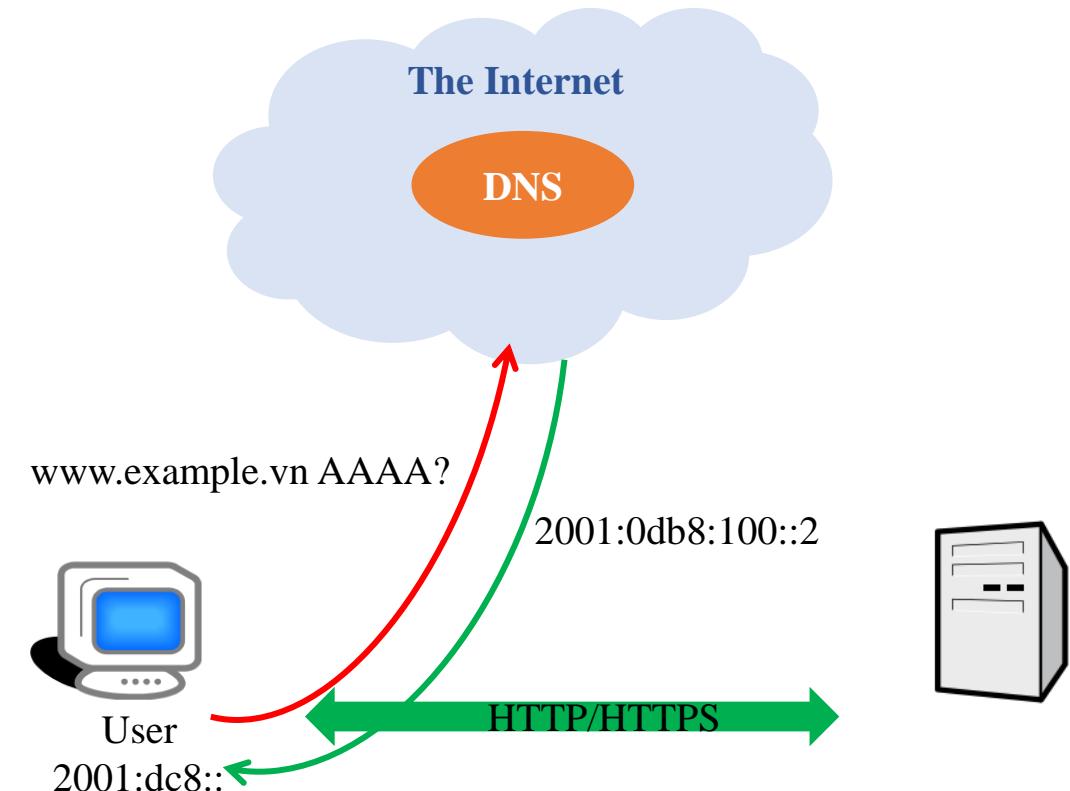
## ❖ Tự quản lý hệ thống máy chủ Webserver

### ➤ Yêu cầu:

- ✓ Mạng lưới, nơi đặt máy chủ Webserver đã triển khai & 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

❖ 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

# Cài đặt, cấu hình IPv6 cho Website (tiếp)

## ❖ 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           [Địa chỉ IPv6 của Website]: Cổng giao thức  
<VirtualHost [2001:0db8:100::2]:80>  
    ServerName www.example.vn          ← Tên miền/ tên Website  
    # ...  
</VirtualHost>
```

- Khởi động lại dịch vụ Apache Server  
service httpd restart

# Cài đặt, cấu hình IPv6 cho Website (tiếp)

## ❖ 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
```

# PHẦN I: HỆ THỐNG DNS

## ➤ 1.1. Lý thuyết hệ thống DNS

- ✓ Hệ thống DNS là gì?
- ✓ Các loại máy chủ DNS
- ✓ File dữ liệu và bản ghi tên miền
- ✓ Hoạt động của hệ thống DNS
- ✓ Cài đặt và cấu hình hệ thống DNS
- ✓ Quản trị và gỡ lỗi DNS
- ✓ An toàn và tối ưu hệ thống DNS

## ➤ 1.2. DNS hoạt động IPv6

- ✓ Quá trình truy vấn, phân giải
- ✓ Khuyến nghị cho DNS hoạt động IPv6
- ✓ Hướng dẫn triển khai DNS hoạt động IPv6
- ✓ Chuyển đổi Website IPv6
- ✓ Khuyến nghị triển khai

## ➤ 1.3. DNSSEC

- ✓ **Nguyên tắc an toàn an ninh hệ thống DNS**
- ✓ **Tấn công hệ thống DNS**
- ✓ **DNSSEC**
- ✓ **DNSSEC hoạt động như thế nào?**
- ✓ **Hoạt động truy vấn DNSSEC**
- ✓ **Các bản ghi tài nguyên mới**
- ✓ **Chain of Trust**
- ✓ **Triển khai DNSSEC trên hệ thống DNS Root**

## ➤ 1.4. Xác thực thư điện tử Email Authentication

- ✓ **Hệ thống thư điện tử (Email)**
- ✓ **Các mối đe dọa trong giao thư điện tử**
- ✓ **Email Authentication**
- ✓ **Giải pháp SPF**
- ✓ **Giải pháp DKIM**
- ✓ **Giải pháp DMARC**

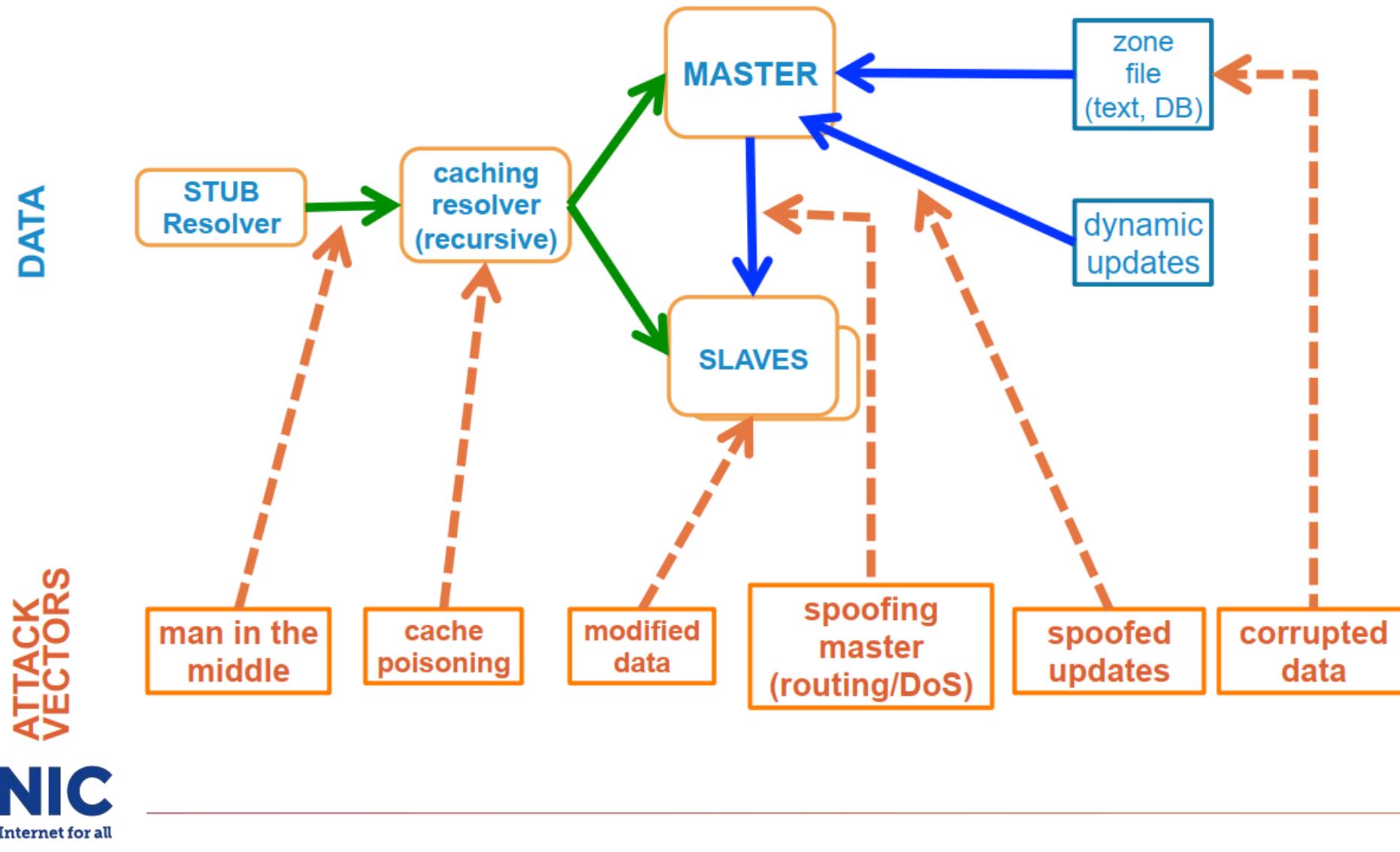
# PHẦN 1: HỆ THỐNG DNS

## DNSSEC

# Nguy cơ an toàn an ninh hệ thống DNS

- ❖ DNS là hệ thống quan trọng
- ❖ DNS là mục tiêu của các cuộc tấn công nhằm chuyển hướng người dùng
- ❖ Giao thức DNS ra đời từ lâu, lỗ hổng bảo mật.

# Nguy cơ an toàn an ninh hệ thống DNS



# 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 là công nghệ an toàn mở rộng của hệ thống DNS, ra đời nhằm các mục đích sau:
  - **Sender authentication:** chứng thực dữ liệu trong quá trình gửi đi.
  - **Data Integrity:** toàn vẹn dữ liệu trong quá trình truyền.
  - **Authenticated denial of existence:** 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.

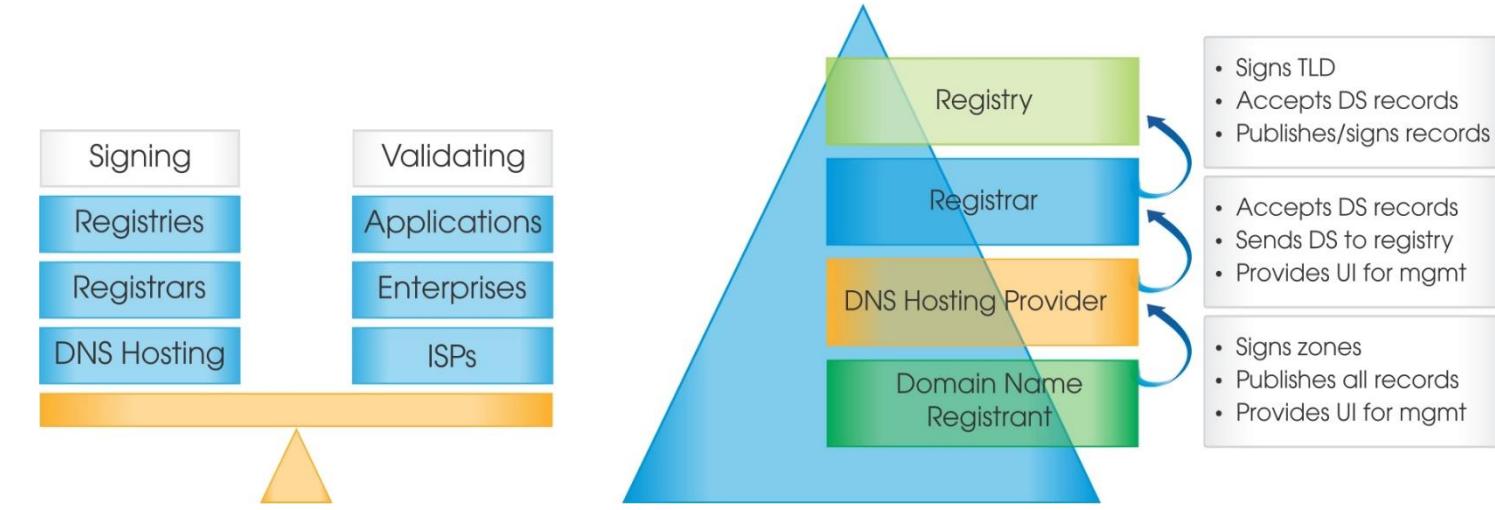
# DNSSEC hoạt động như thế nào?

## ❖ Các máy chủ DNS Authoritative

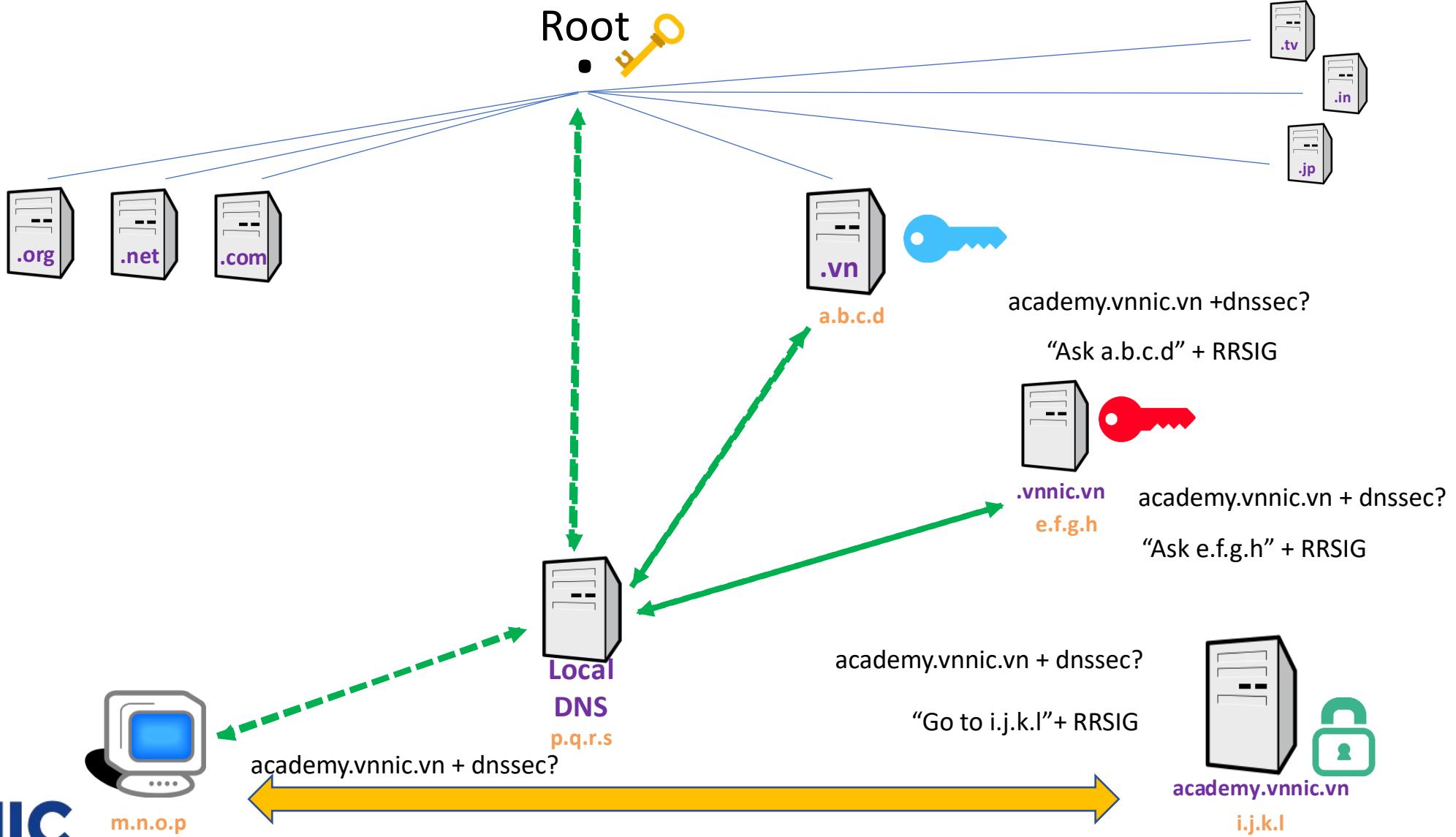
- Ký DNSSEC cho các zone tên miền
- Phản hồi các truy vấn được truy vấn đồng thời gửi kèm bản ghi chữ ký RRSIG trong phản hồi truy vấn

## ❖ 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”



# Hoạt động truy vấn DNSSEC



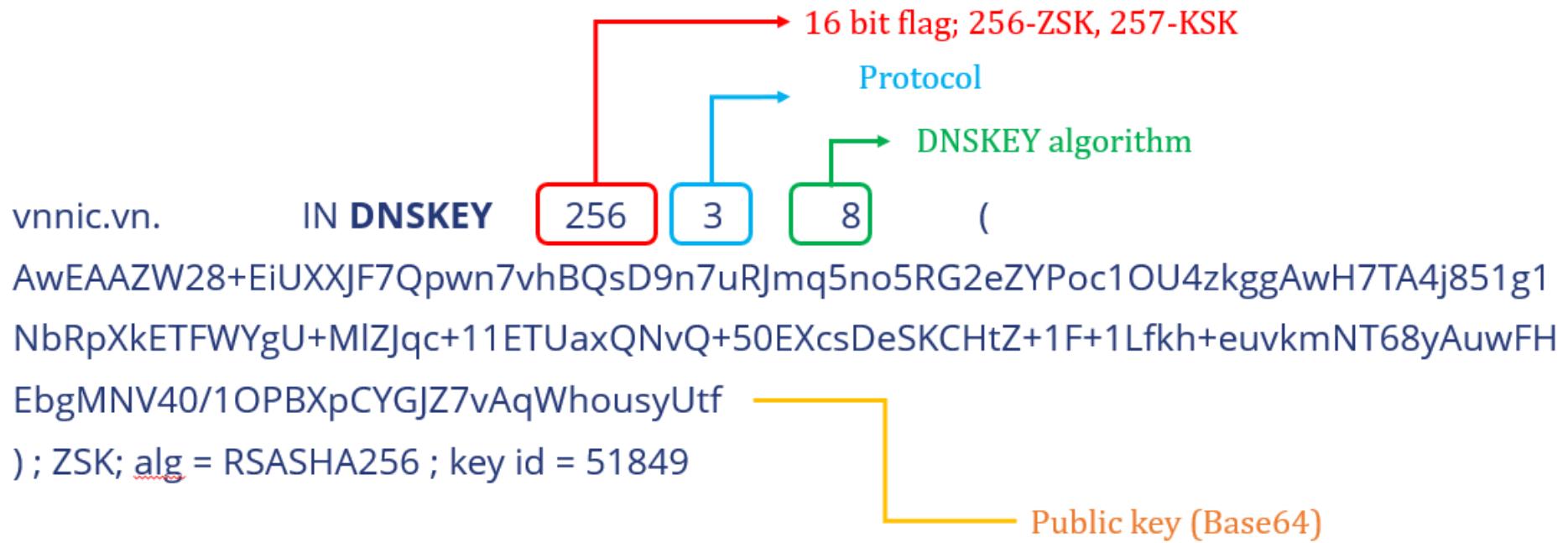
# Các bản ghi tài nguyên mới

Bản ghi	Mô tả/ chức năng	
<b>RRSIG</b>	Resource Record Signature – Bản ghi chữ ký tài nguyên	sử dụng để chứng thực cho các bản ghi tài nguyên trong zone dữ liệu.
<b>DNSKEY</b>	DNS Key	sử dụng để xác thực bản ghi RRSIG
<b>DS</b>	Delegation Signer	thiết lập chứng thực giữa các zone dữ liệu, sử dụng trong việc ký xác thực trong quá trình chuyển giao DNS.
<b>NSEC / NSEC3</b>	Next Secure	Xác định các tên miền tiếp theo trong zone. Xác thực từ chối sự tồn tại của các tên miền không tồn tại.

# Các bản ghi tài nguyên mới

## ❖ Bản ghi DNSKEY

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



# Các bản ghi tài nguyên mới

## ❖ Bản ghi DNSKEY

- 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)

# Các bản ghi tài nguyên mới

## ❖ Bản ghi DNSKEY

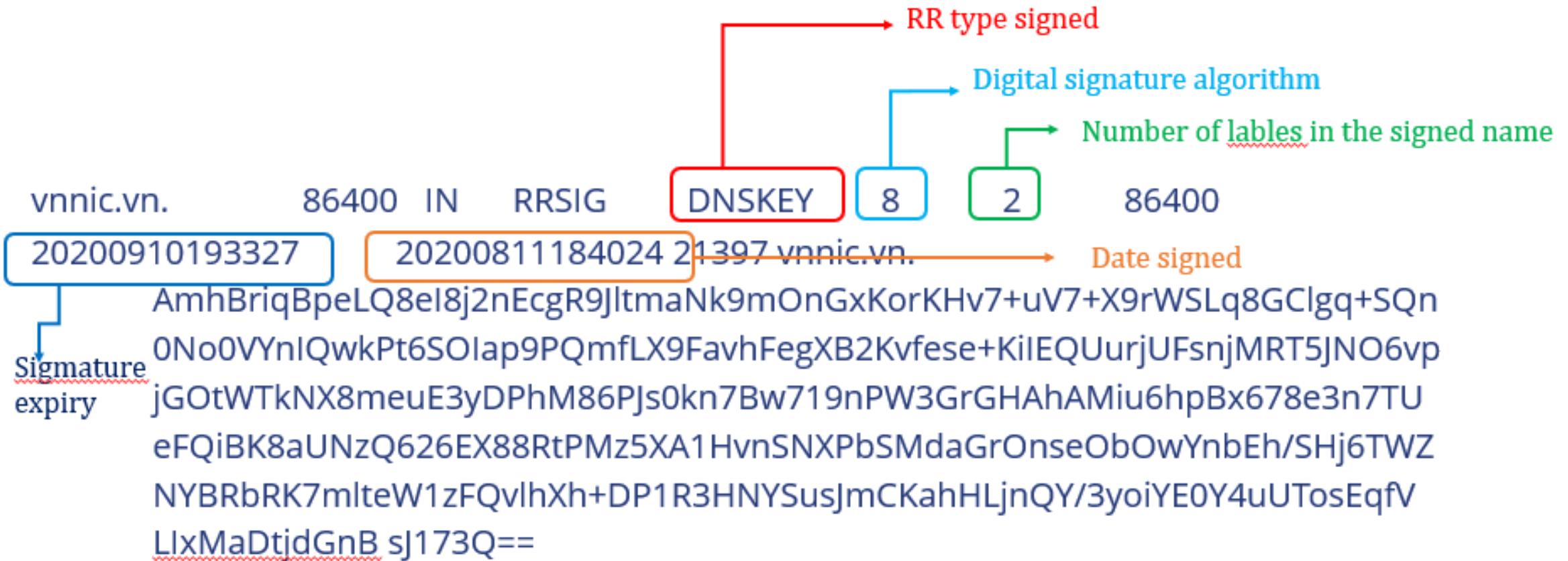
### ➤ KSK và ZSK

- ✓ 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
<ul style="list-style-type: none"><li>- KSK dùng để ký bản ghi DNSKEY trong một zone.</li><li>- KSK luôn có odd flag là 257.</li><li>- Khi KSK thay đổi, bản ghi DS trong parent zone phải được update.</li><li>- KSK thường được tạo với kích thước lớn để chống lại các tấn công brute force.</li><li>- KSK thường có thời gian sống (lifetime) lâu</li></ul>	<ul style="list-style-type: none"><li>- ZSK được 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.</li><li>- ZSK luôn có odd flag là 256.</li><li>- Khi ZSK thay đổi, không cần thiết phải thay đổi bản ghi DS trên parent zone.</li><li>- ZSK thường có thời gian sống ngắn hơn, và được “rolled” nhiều hơn.</li></ul>

# Các bản ghi tài nguyên mới

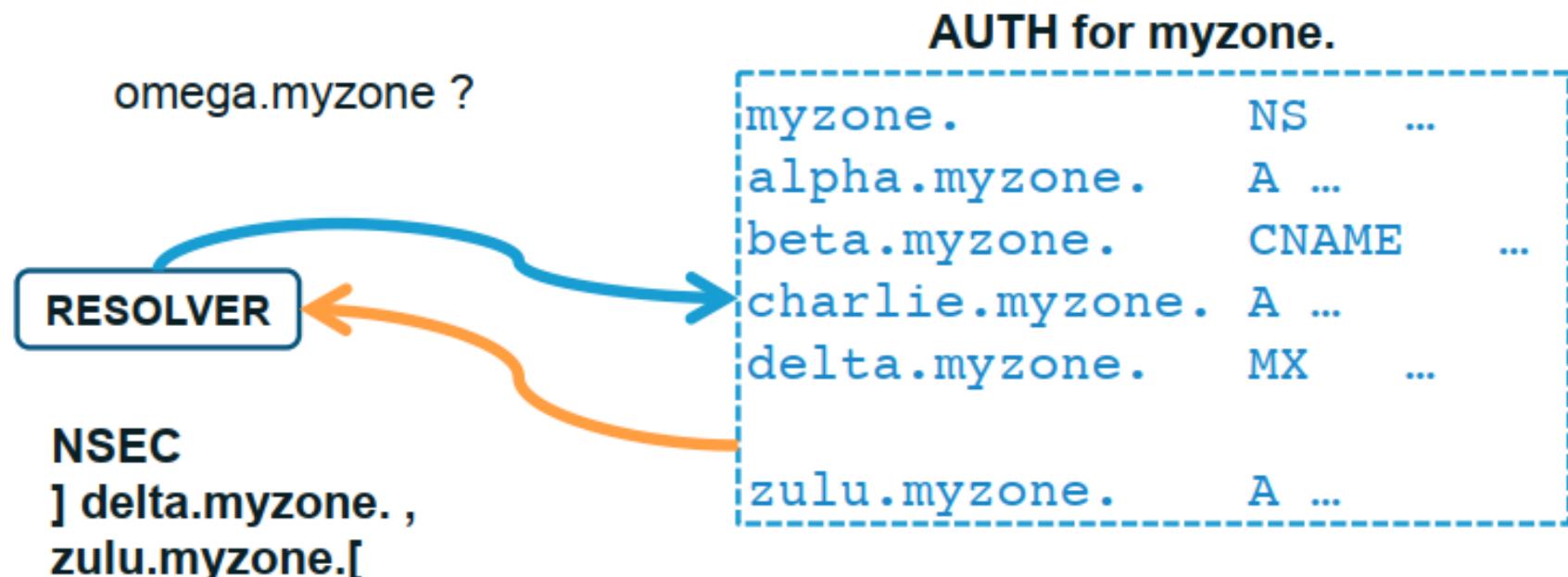
## ❖ Bản ghi RRSIG



# Các bản ghi tài nguyên mới

## ❖ Bản ghi NSEC (Next Secure)

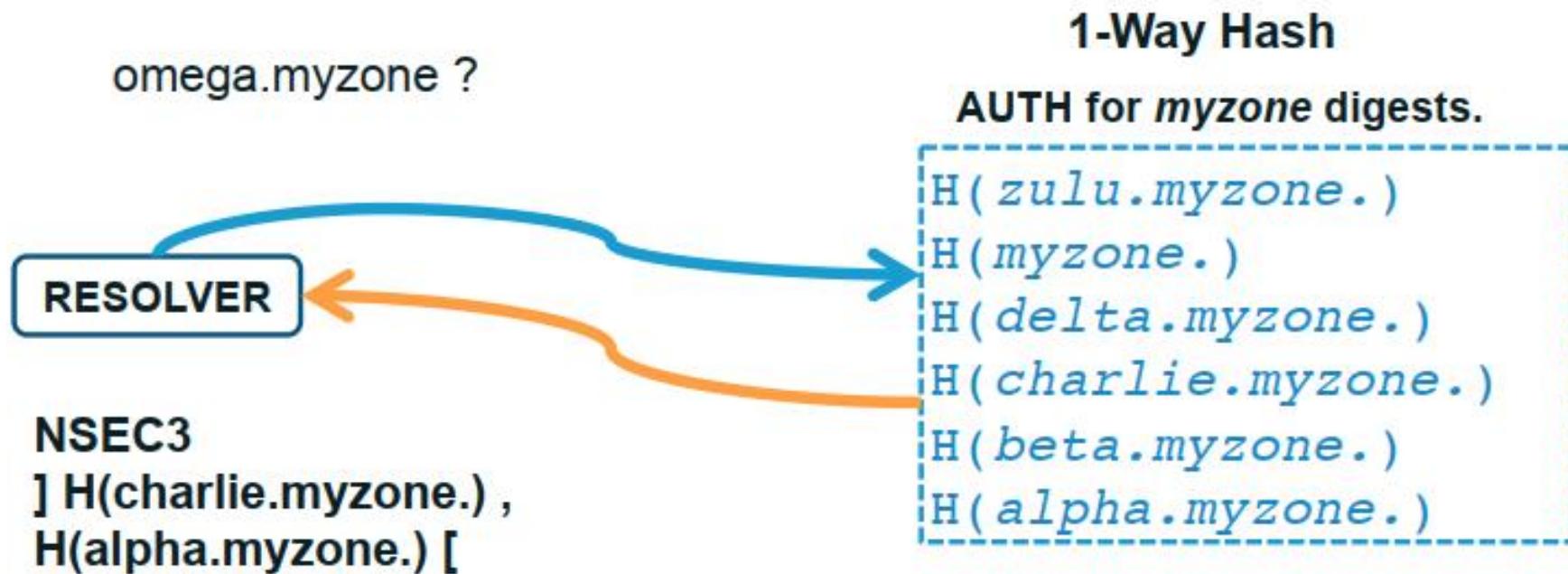
- Tạo thành một chuỗi các tên miền kế tiếp nhau trong zone
- Xác thực từ chối sự tồn tại của các tên miền NXDomains (không tồn tại)



# Các bản ghi tài nguyên mới

## ❖ Bản ghi NSEC3

- 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”



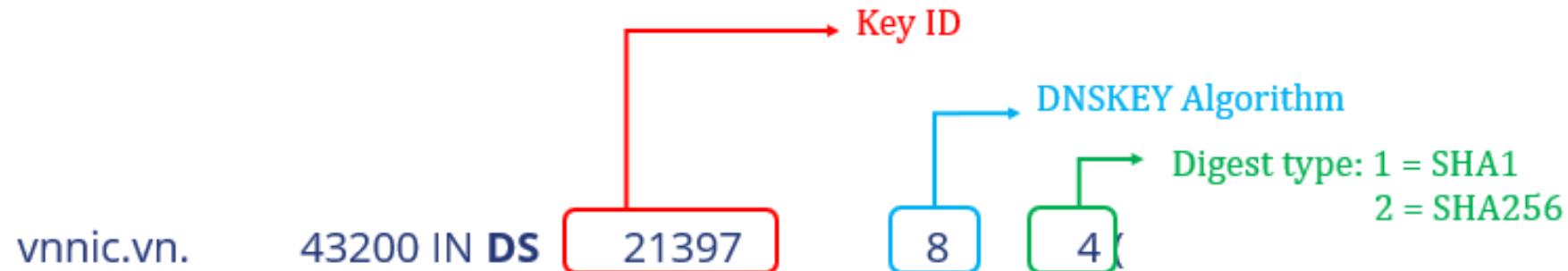
# Các bản ghi tài nguyên mới

## ❖ **Bản ghi DS (Delegation Signer)**

- 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.

# Các bản ghi tài nguyên mới

## ❖ Bản ghi DS (Delegation Signer)



6DB019A715A251627308A543365ED85C2E2350D72BEA

ACE00C1F580E8D66471D6FA1FF080D74BE8A878E5C71  
B2C8A0F9 )

- ❖ 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 của child.
  - DNSKEY của child zone được ký bằng KSK của chính nó.

# Chain of Trust

**DNSSEC.vn** 



**DNS Caching  
của các ISP**

(VDC/VNPT, VIETTEL, FPT,...)

**.VN Top level DNS server**

(Registry: VNNIC)  
Registrar, DNS Hosting Provider, DNS Owner  
PAVN, FPT, MATBAO, VDC/VNPT,...)



**ROOT**

 **DNSKEY root**  
 **DS .vn**



 **DNSKEY .vn**  
 **DS example.vn**



 **DNSKEY example.vn**

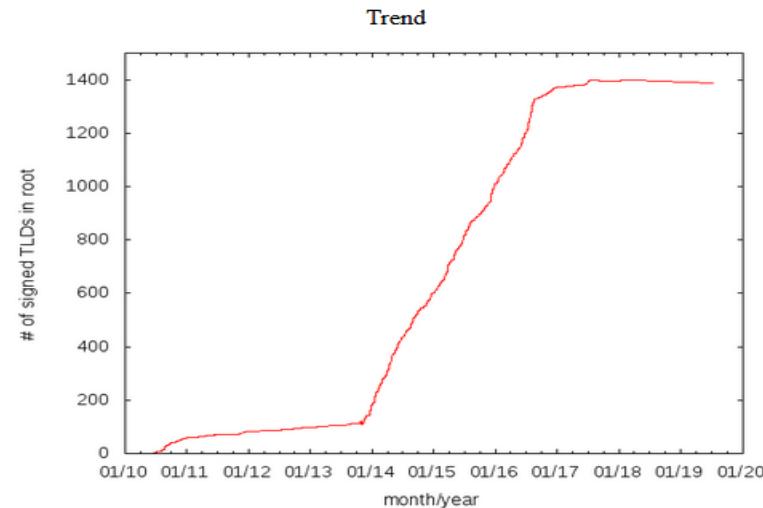
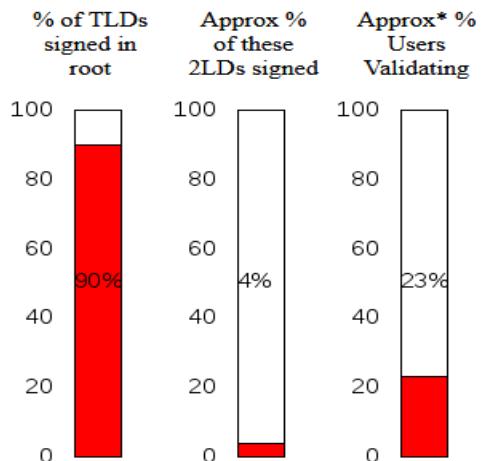
**.VN Second level DNS server**

(Registrar, DNS Hosting Provider, DNS Owner  
PAVN, FPT, MATBAO, VDC/VNPT,...)

<https://vnnic.vn>

# Triển khai DNSSEC trên hệ thống DNS Root

- ❖ Hiện tại có 1389/1514 tên miền cấp cao (TLD) đã triển khai DNSSEC (tính đến tháng 06/2020)
- ❖ Khoảng 50% tên miền cấp cao mã quốc gia (ccTLD) đã triển khai DNSSEC
- ❖ Root DNS KSK Rollover: 11/10/2018

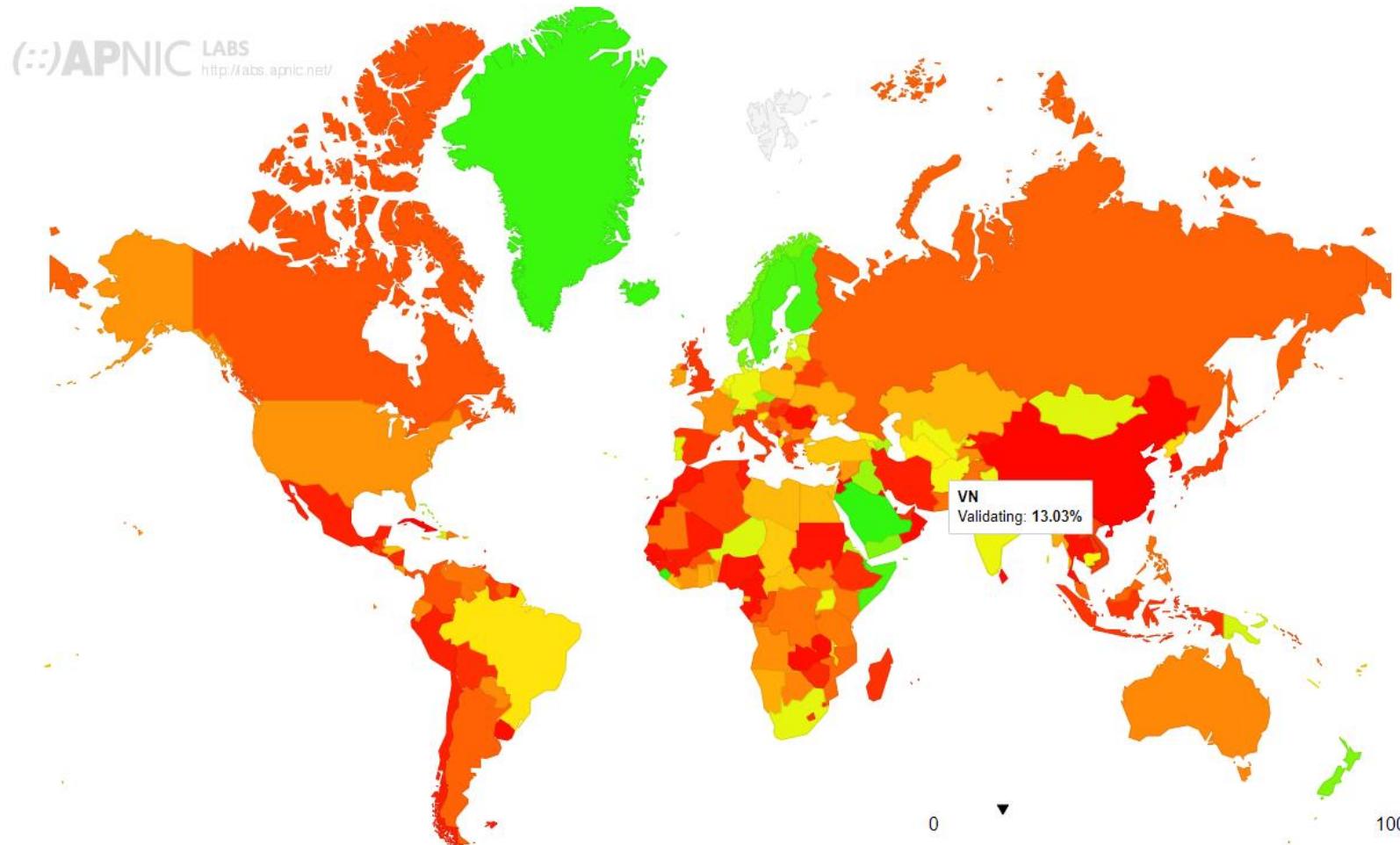


Tỷ lệ triển khai DNSSEC cho các TLD/2LD trên thế giới

Triển khai DNSSEC ccTLD

# DNSSEC Validation Rate

DNSSEC Validation Rate by country (%)



# PHẦN I: HỆ THỐNG DNS

## ➤ 1.1. Lý thuyết hệ thống DNS

- ✓ chủ DNS
- ✓ Hệ thống DNS là gì?
- ✓ Các loại máy liệu và bản ghi tên miền
- ✓ Hoạt động của hệ thống DNS
- ✓ Cài đặt và cấu hình hệ thống DNS
- ✓ Quản trị và gỡ lỗi DNS
- ✓ An toàn và tối ưu hệ thống DNS

## ➤ 1.2. DNS hoạt động IPv6

Qúa trình truy vấn, phân giải

- ✓ Khuyến nghị cho DNS hoạt động IPv6
- ✓ Hướng dẫn triển khai DNS hoạt động IPv6
- ✓ Chuyển đổi Website IPv6
- ✓ Khuyến nghị triển khai

## ➤ 1.3. DNSSEC

Nguyên cơ an toàn an ninh hệ thống DNS

- ✓ Tấn công hệ thống DNS
- ✓ DNSSEC
- ✓ DNSSEC hoạt động như thế nào?
- ✓ Hoạt động truy vấn DNSSEC
- ✓ Các bản ghi tài nguyên mới
- ✓ Chain of Trust
- ✓ Triển khai DNSSEC trên hệ thống DNS Root

## ➤ 1.4. Xác thực thư điện tử

Email Authentication

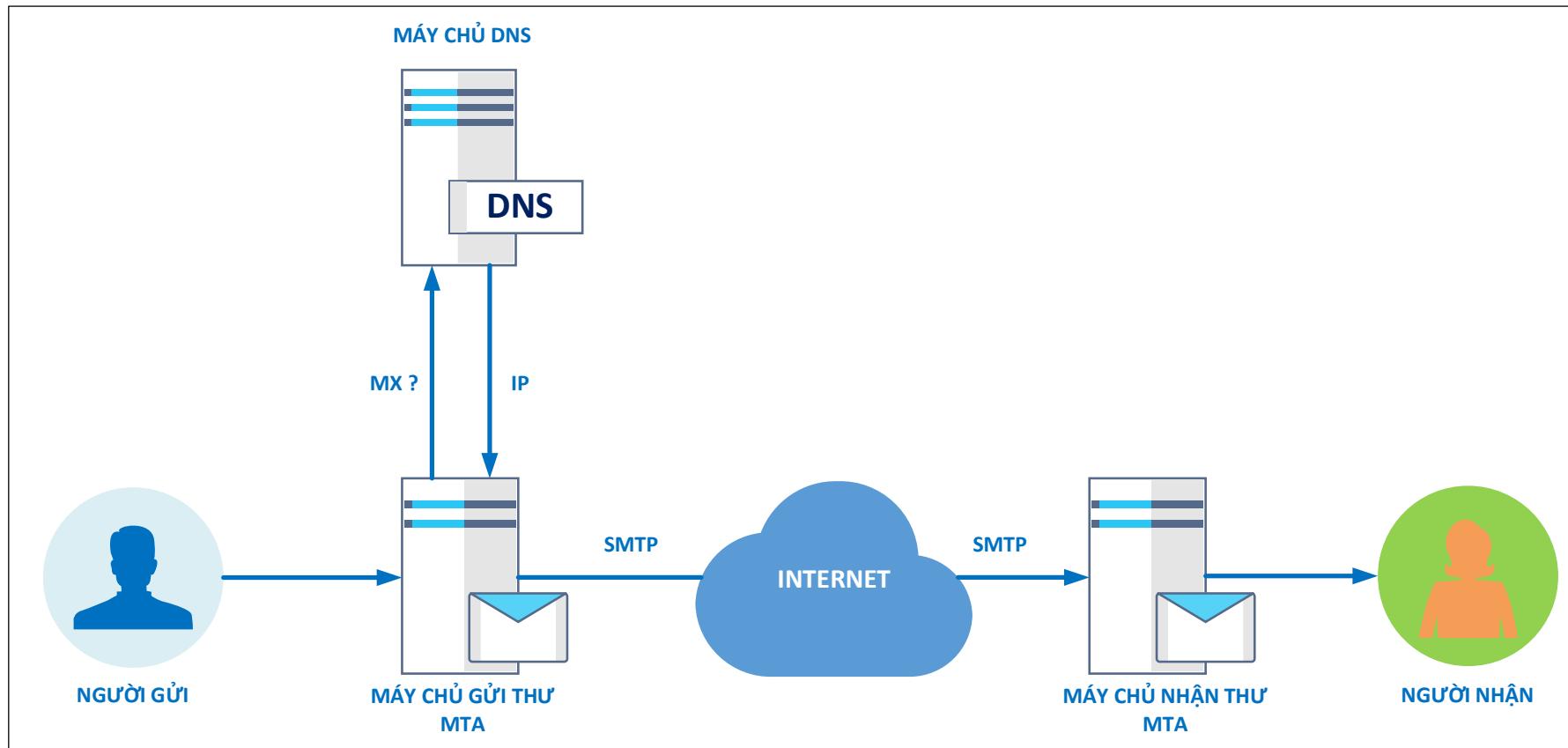
Hệ thống thư điện tử (Email)

- ✓ Hệ thống thư điện tử (Email)
- ✓ Các mối đe dọa trong giao thư điện tử
- ✓ Email Authentication
- ✓ Giải pháp SPF
- ✓ Giải pháp DKIM
- ✓ Giải pháp DMARC

## XÁC THỰC THƯ ĐIỆN TỬ EMAIL AUTHENTICATION HỆ THỐNG THƯ ĐIỆN TỬ (EMAIL)

# Hệ thống thư điện tử (Email)

- ❖ Thư điện tử (email hay e-mail) là một phương thức trao đổi thông điệp/thông tin giữa những người sử dụng các thiết bị điện tử.
- ❖ Thư điện tử hoạt động qua các mạng máy tính mà hiện nay chủ yếu là mạng Internet.
- ❖ Giao thức SMTP là giao thức truyền thư đơn giản, là một chuẩn giao thức Internet dùng trong việc gửi thư điện tử.



# Hiện trạng sử dụng Email hiện nay trên thế giới

- ❖ Số lượng người dùng Email trên thế giới tính từ thời điểm năm 2015 đến năm 2019

	2015	2016	2017	2018	2019
<b>Worldwide Email Accounts (M)</b>	4,353	4,626	4,920	5,243	5,594
<i>%Growth</i>		6%	6%	7%	7%
<b>Worldwide Email Users* (M)</b>	2,586	2,672	2,760	2,849	2,943
<i>% Growth</i>		3%	3%	3%	3%
<b>Average Accounts Per User</b>	1.7	1.7	1.8	1.8	1.9

Table 1: Worldwide Email Accounts and User Forecast (M), 2015–2019

<https://www.radicati.com/wp/wp-content/uploads/2015/02>Email-Statistics-Report-2015-2019-Executive-Summary.pdf>

# Hiện trạng sử dụng Email hiện nay trên thế giới

- ❑ Lưu lượng trao đổi Email (Email traffic) mỗi ngày trên thế giới (số liệu thống kê từ năm 2015 đến năm 2019)

Daily Email Traffic	2015	2016	2017	2018	2019
<b>Total Worldwide Emails Sent/Received Per Day (B)</b>	<b>205.6</b>	<b>215.3</b>	<b>225.3</b>	<b>235.6</b>	<b>246.5</b>
<i>% Growth</i>	5%	5%	5%	5%	5%
<b>Business Emails Sent/Received Per Day (B)</b>	<b>112.5</b>	<b>116.4</b>	<b>120.4</b>	<b>124.5</b>	<b>128.8</b>
<i>% Growth</i>	3%	3%	3%	3%	3%
<b>Consumer Emails Sent/Received Per Day (B)</b>	<b>93.1</b>	<b>98.9</b>	<b>104.9</b>	<b>111.1</b>	<b>117.7</b>
<i>% Growth</i>	6%	6%	6%	6%	6%

Table 2: Worldwide Daily Email Traffic (B), 2015-2019

<https://www.radicati.com/wp/wp-content/uploads/2015/02>Email-Statistics-Report-2015-2019-Executive-Summary.pdf>

# Các mối đe dọa trong giao dịch thư điện tử

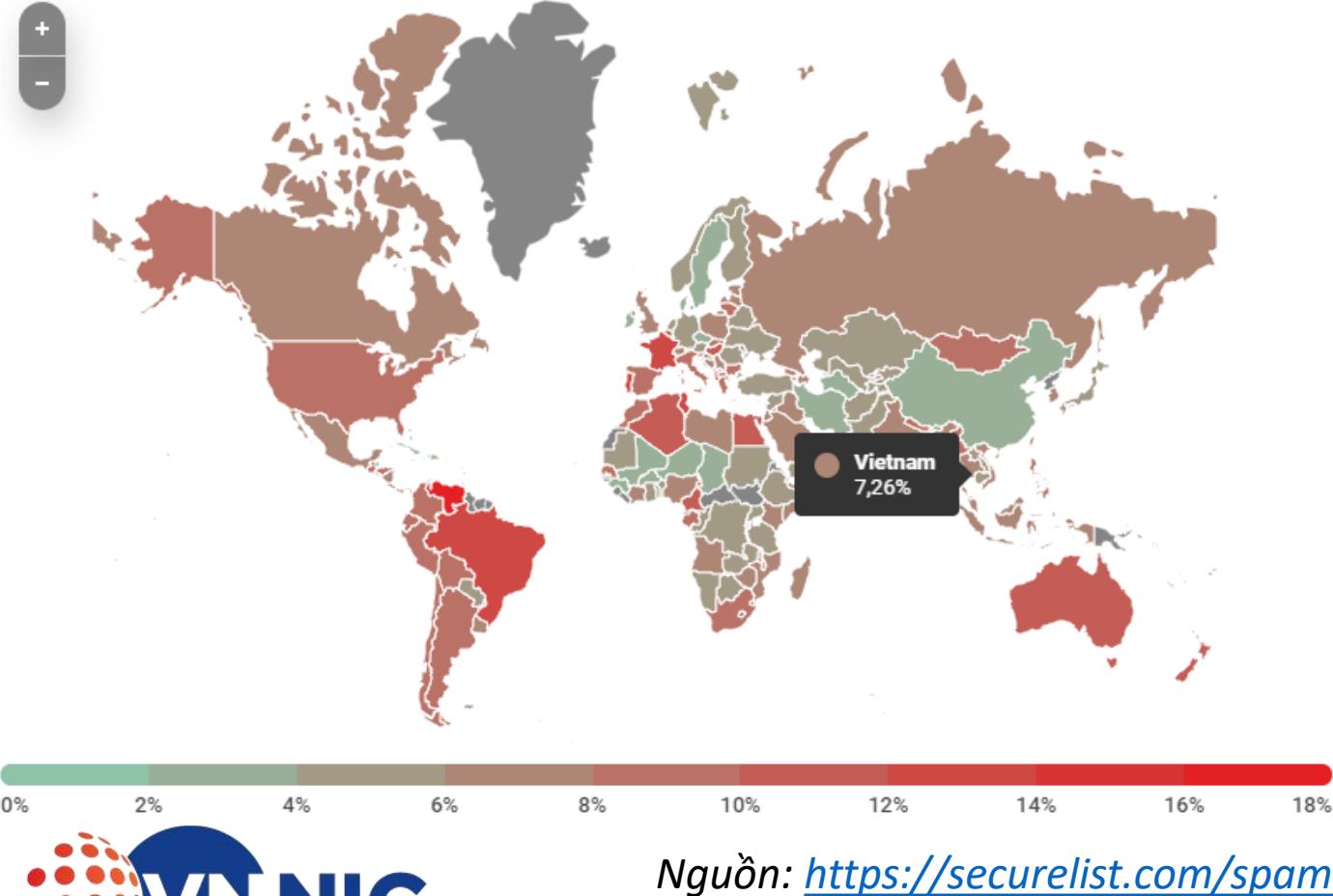
## ❖ Các hình thức tấn công qua hệ thống thư điện tử

- **Thư điện tử giả mạo (phising mail):** là hình thức lừa đảo trực tuyến được thực hiện trực tiếp bởi các nhóm tội phạm và kẻ tấn công. Chúng lợi dụng sự thiếu hiểu biết của người dùng để nhắm khai thác các thông tin nhạy cảm như mật khẩu, tài khoản ngân hàng và số thẻ tín dụng của người dùng
- **Thư rác (spam mail):** Các thư điện tử này thường chứa các loại quảng cáo được gửi một cách vô tội vạ và nơi nhận là một danh sách cá nhân và nhóm người dùng, các dạng thư này thường vô bổ và không có chất lượng thông tin.
- **Phần mềm độc hại:** đó là các thư điện tử vẫn đang được sử dụng như một trong những phương pháp chính để lây lan và phát tán các mối đe dọa máy tính như các phần mềm độc hại: virus, mã độc, ransomware.... Và các phần mềm độc hại cũng sử dụng thư điện tử như công cụ để phát tán chính mình.

# Các mối đe dọa trong giao dịch thư điện tử

## ❖ Phishing mail

➤ Nguồn email phishing theo quốc gia (Q2/2020):



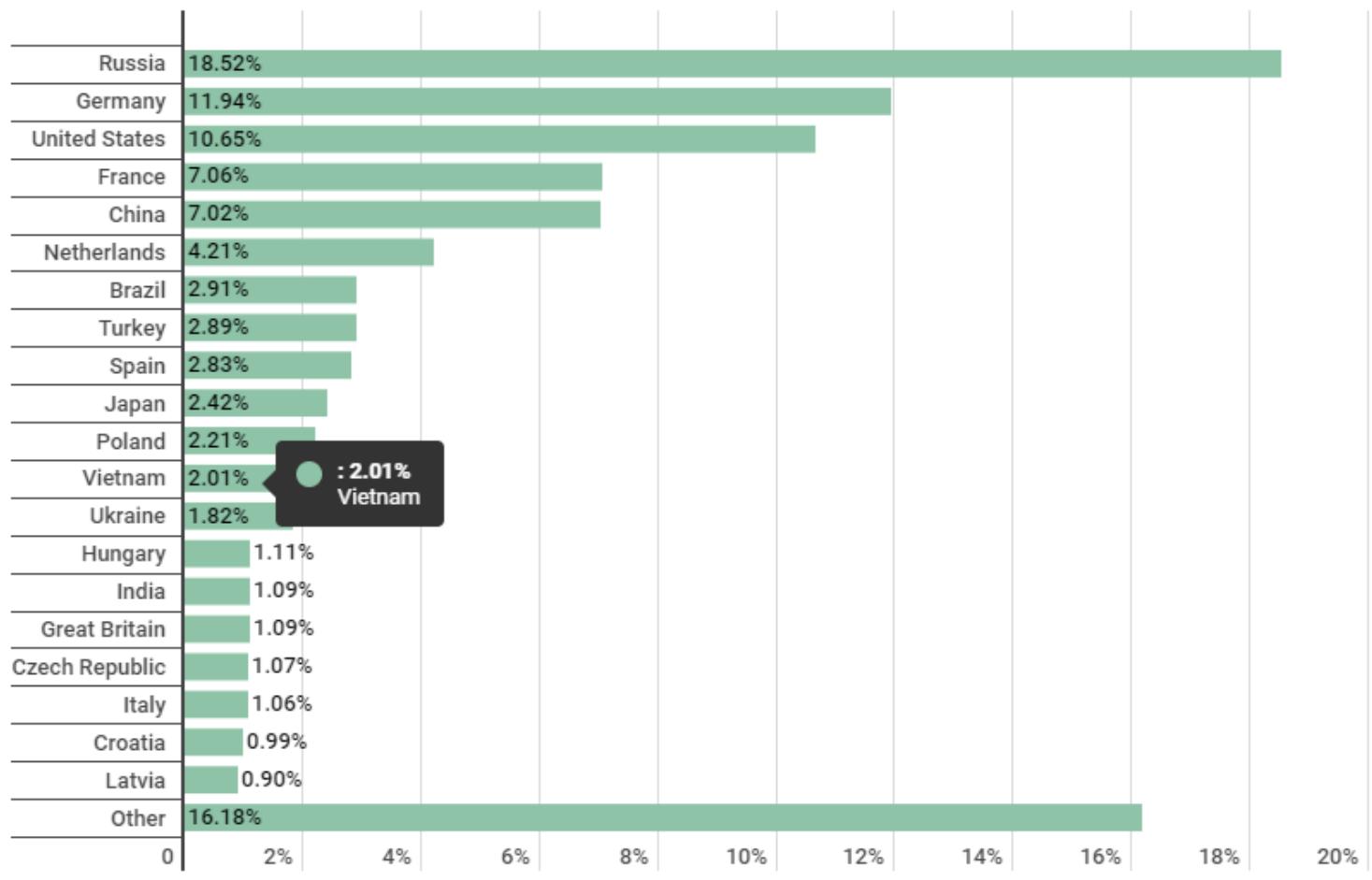
Nguồn: <https://securelist.com/spam-and-phishing-in-q2-2020/97987/>

# Các mối đe dọa trong giao dịch thư điện tử

## ❖ Spam mail

- Nguồn email spam theo quốc gia (Q2/2020):

Sources of spam by country



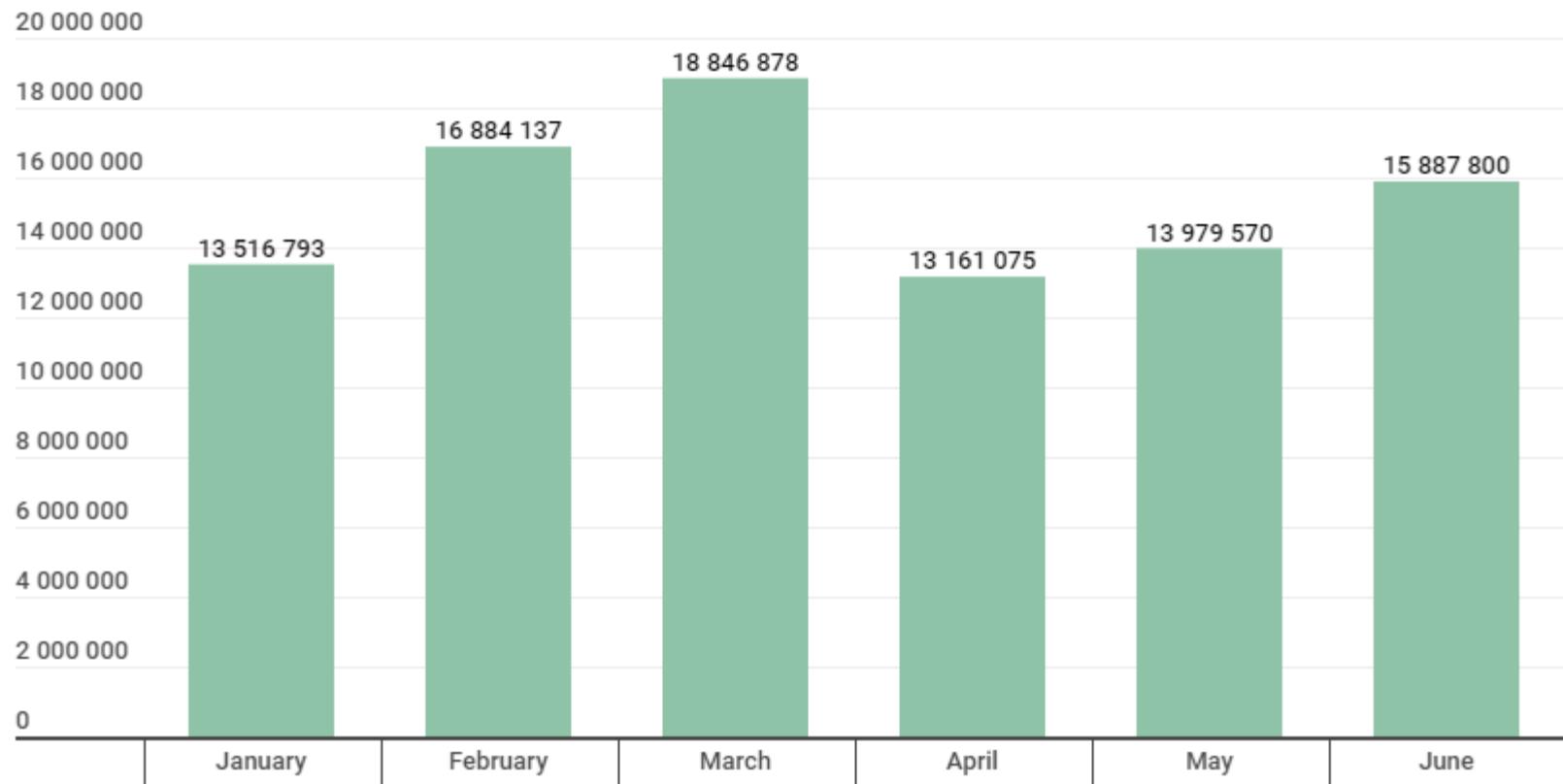
Nguồn: <https://securelist.com/spam-and-phishing-in-q2-2020/97987/>

# Các mối đe dọa trong giao dịch thư điện tử

## ❖ Phần mềm độc hại

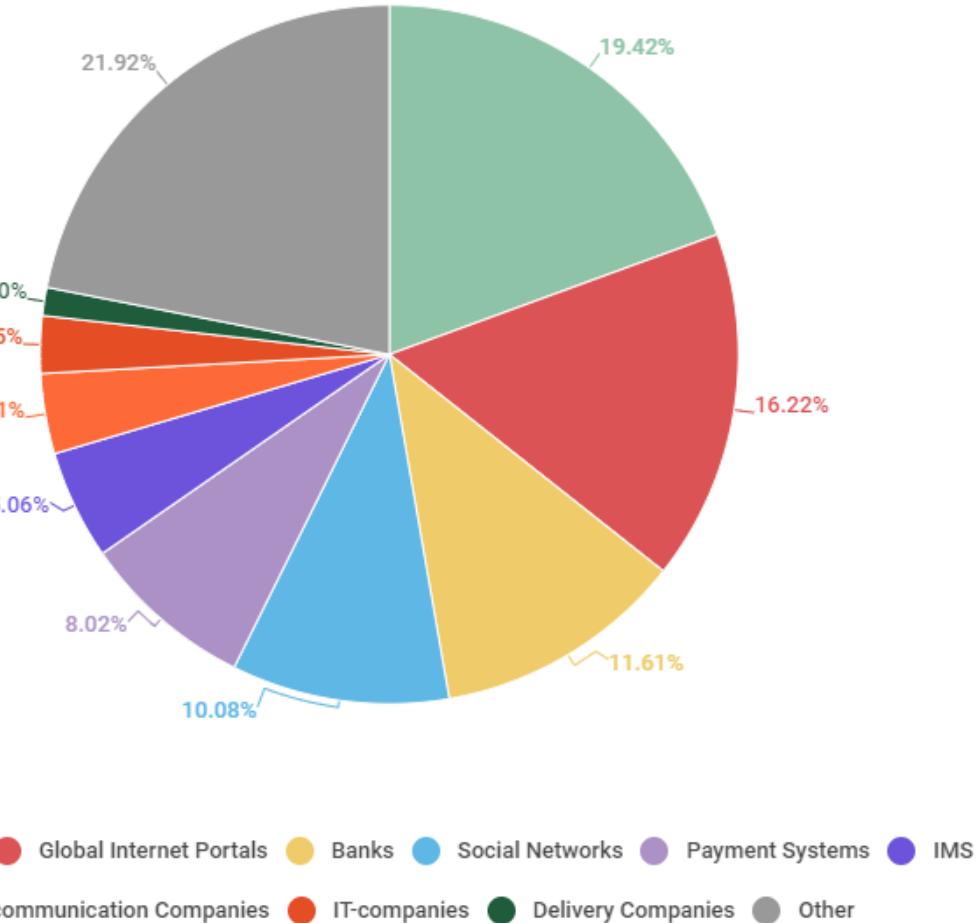
- Phần mềm độc hại đính kèm theo email (Q2/2020):

**Malicious attachments: malware families**



# Các mối đe dọa trong giao dịch thư điện tử

- ❖ Đối tượng bị tấn công (Q2/2020)
  - Tập trung chủ yếu vào các đối tượng lĩnh vực:
    - ✓ Online Stores
    - ✓ Global Internet Portals
    - ✓ Banks
    - ✓ Social Networks



Nguồn: <https://securelist.com/spam-and-phishing-in-q2-2020/97987/>

# Email Authentication

- ❖ Email Authentication: Xác thực Email
- ❖ Gồm các giải pháp công nghệ nhằm xác thực người gửi email chính xác đến từ đâu:
  - Các giải pháp công nghệ này hầu hết được triển khai trên hạ tầng hệ thống Email và người dùng cuối (end-user) không nhận thấy điều đó.
  - Tất cả các giải pháp này đều có điểm mạnh và tồn tại các điểm yếu.
  - Không có giải pháp nào đảm bảo hoàn toàn 100%.

## ❖ Các giải pháp xác thực Email

- Có 3 giải pháp xác thực Email chính và sử dụng phổ biến:
  - ✓ SPF - Sender Policy Framework (2003)
    - IETF Status: Standards Track RFC
    - <http://www.openspf.org>
  - ✓ DKIM – Domain Keys Identified Message (2007)
    - IETF Status: Standards Track RFC
    - <http://opendkim.org>
  - ✓ DMARC – Domain-based Message Authentication, Reporting, and Conformance (2012)
    - IETF Status: Informational RFC, Working Group
    - <http://dmarc.org>
- Một số giải pháp xác thực email khác:
  - ✓ Sender-ID – Combination of SPF and Caller ID proposals
  - ✓ ADSP - Author Domain Signing Practices

# Giải pháp xác thực thư điện tử SPF

## ❖ Sender Policy Framework (SPF)

- Phương pháp xác thực sử dụng SPF là sử dụng bản ghi SPF được khai báo trên DNS để xác thực địa chỉ IP của máy chủ gửi thư phía người gửi chính là từ chủ sở hữu tên miền. Đây là một trong những phương pháp đơn giản, cung cấp thông tin cho các MTA phía người nhận có thể kiểm tra xác thực MTA từ phía người gửi, qua đó có những hành động chặn lọc phù hợp với chính sách của tổ chức.
- Mục đích của việc sử dụng bản ghi SPF là để ngăn chặn những kẻ mạo danh gửi thư điện tử với địa chỉ giả mạo sử dụng tên miền của các cơ quan, tổ chức. Người nhận có thể tham chiếu bản ghi SPF để xác định liệu rằng thư điện tử được gửi từ máy chủ thư điện tử được ủy quyền từ tên miền của người gửi.

# Giải pháp xác thực thư điện tử SPF

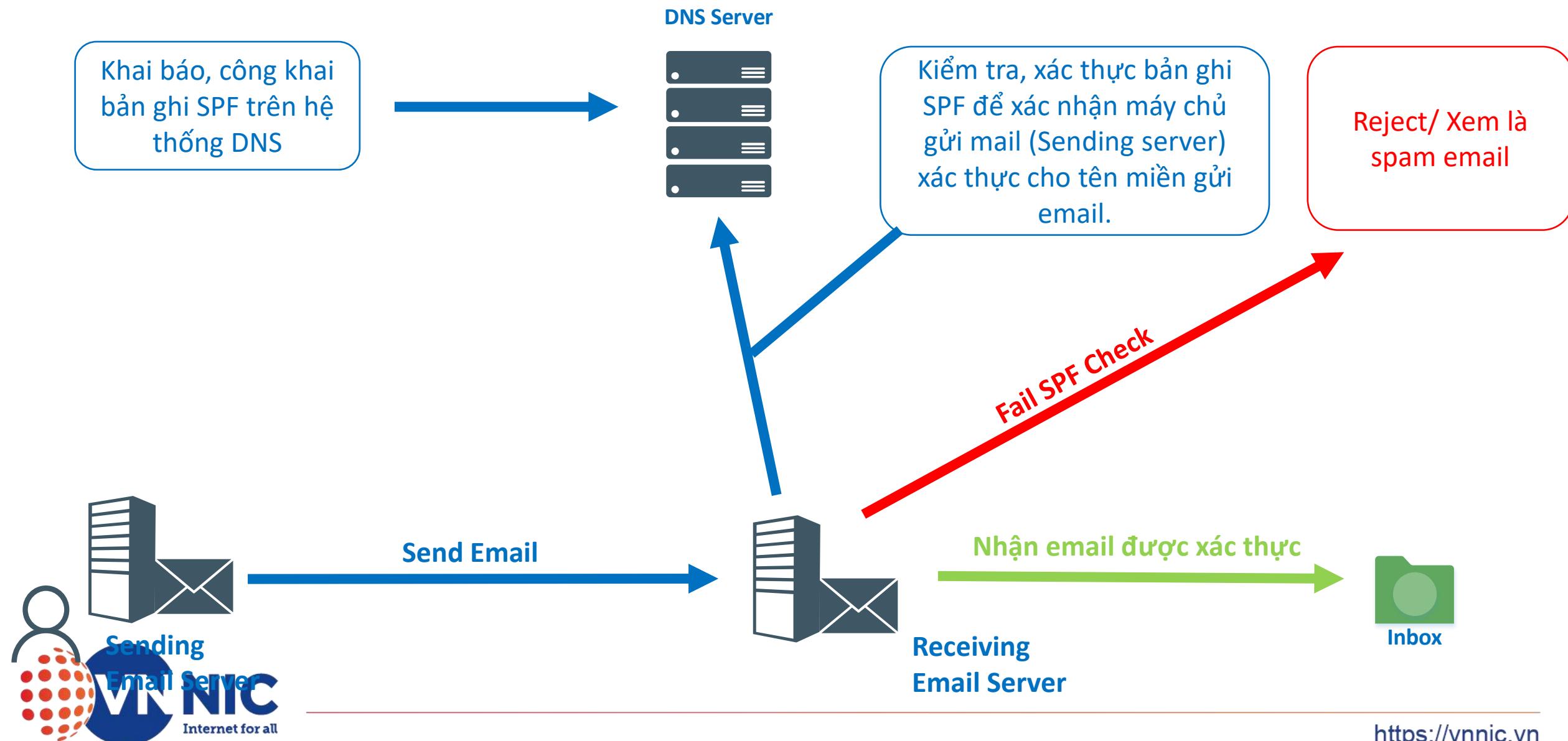
## ❖ Bên gửi mail:

- Các máy chủ mail của bên gửi sẽ thực hiện khai báo thông tin mail tương ứng của các tên miền (domain) chỉ được gửi chính xác từ các máy chủ mail có địa chỉ xác định bằng cách khai báo trong bản ghi TXT trên hệ thống DNS.

## ❖ Bên nhận mail:

- Khi nhận được mail từ phía người gửi, máy chủ mail bên nhận sẽ truy vấn DNS bản ghi TXT tương ứng của tên miền có các thư điện tử bên gửi, xác thực thông tin địa chỉ IP của máy chủ mail bên gửi. Nếu thông tin chính xác thì sẽ xác nhận mail, nếu không sẽ đưa vào các thư mục spam, xem xét (phụ thuộc vào chính sách của bên nhận).

# Giải pháp xác thực thư điện tử SPF



# Giải pháp xác thực thư điện tử SPF

## ❖ Bản ghi SPF

- Cú pháp: ***example.vn IN TXT "v=spf1 a:mail.example.vn -all"***
- Identifier tag: v=spf1
- Các tham số:

a	Kiểm tra máy chủ tương ứng với tên hostname
mx	Kiểm tra máy chủ tương ứng với bản ghi MX
ipv4	Kiểm tra máy chủ tương ứng với địa chỉ IPv4
Ipv6	Kiểm tra máy chủ tương ứng với địa chỉ IPv6
Exists	Kiểm tra máy chủ với một macro
ptr	Không sử dụng

# Giải pháp xác thực thư điện tử SPF

## ❖ Tham số

Mechanisms	Results
+	Pass
-	Fail
~	Softfail
?	Neutral
+all	Pass all matches
-all	Fail all matches
~all	Softfail all matches
?all	Neutral all matches

# Giải pháp xác thực thư điện tử SPF

## ❖ Giá trị kết quả

Result	Giải thích	Hành động
Pass	Bản ghi SPF chỉ định máy chủ được phép gửi thư	Accept
Fail	Bản ghi SPF chỉ định máy chủ không được phép gửi thư	Reject
Softfail	Bản ghi SPF chỉ định máy chủ không được phép gửi thư nhưng được phép chuyển tiếp.	Accept but mark
Neutral	Bản ghi SPF chỉ định rõ ràng rằng không xét về tính hợp lệ	Accept
None	Tên miền không có bản ghi SPF	Accept

# Giải pháp xác thực thư điện tử SPF

## ❖ Ưu điểm

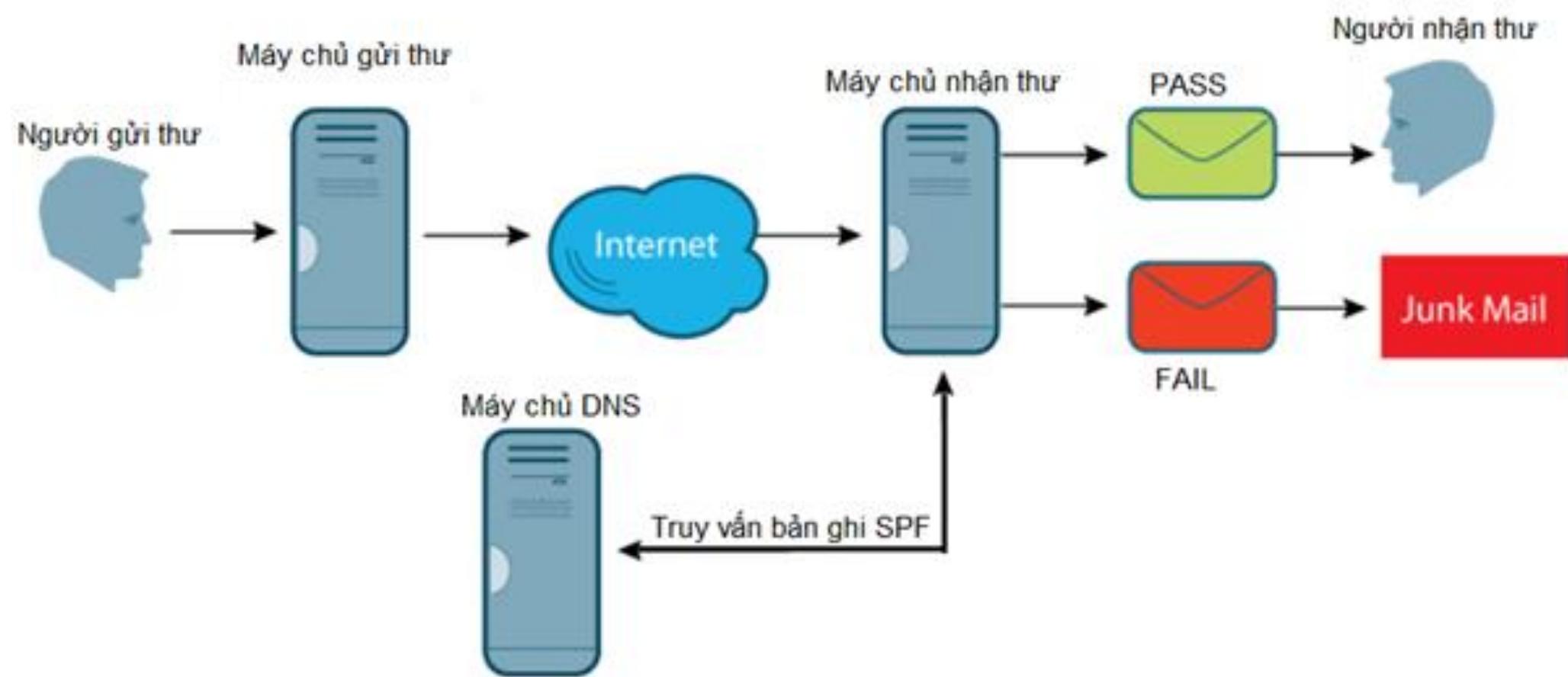
- **Tăng độ tin tưởng** với hệ thống bên nhận hơn khi nhận mail đến từ domain có khai báo SPF.
- **Nhận được sự ưu tiên** của Gmail, Yahoo khi kiểm tra nhờ vào các email gửi từ domain có khai báo SPF.

## ❖ Hạn chế

- SPF không hiệu quả trong việc chuyển tiếp (forwarding) và mailing list.
- Mailing list và trong một số luồng gián tiếp khác có thể bị tác động viết lại RFC5321.MailFrom để tạo và vượt qua SPF check.
- Nhiều người nhận không hoạt động theo đúng chính sách của SPF.

# Giải pháp xác thực thư điện tử SPF

## ❖ Mô hình triển khai



# Giải pháp xác thực thư điện tử SPF

## ❖ Hướng dẫn triển khai:

- Quá trình xác thực thư điện tử bằng SPF sẽ được thực hiện trên tên miền của đơn vị, tổ chức sở hữu tên miền.
- Triển khai phương pháp xác thực thư điện tử bằng giao thức SPF đơn giản chỉ bao gồm việc khai báo bản ghi SPF (bản ghi DNS loại TXT) trên hệ thống DNS hosting tên miền của đơn vị, tổ chức sở hữu tên miền.
- Ví dụ, trên hệ thống DNS hosting tên miền, thực hiện khai báo bản ghi sau:

test-mail.vnnic.vn IN TXT "v=spf1 a mx ip4:10.10.64.128/25 -all"

Tên miền

Loại bản ghi (TXT)

Các tham số SPF policy

# Giải pháp xác thực thư điện tử DKIM

## ❖ DomainKeys Identified Mail (DKIM)

- Giao thức DKIM (DomainKeys Identified Mail) được sử dụng để ngăn chặn sự giả mạo thư điện tử bằng cách thêm một chữ ký số (DKIM Signature) vào phần header (tiêu đề) của các thư điện tử được gửi đi. Giao thức này sử dụng một khóa tên miền riêng tư (private domain key) để mã hóa tiêu đề của thư điện tử, và khai báo một khóa tên miền công khai (public domain key) vào các bản ghi DNS của tên miền đó. Máy chủ nhận thư có thể truy vấn đến tên miền gửi thư để lấy khóa công khai và giải mã nội dung phần tiêu đề của thư, và xác nhận rằng thư điện tử thực sự đến từ tên miền đó và không bị thay đổi trong quá trình truyền.
- DKIM là một giao thức cho phép một cơ quan, tổ chức chịu trách nhiệm cho quá trình truyền thư điện tử theo cách mà các nhà cung cấp dịch vụ thư điện tử có thể xác minh tính hợp lệ của thư đó. Sự xác minh tính hợp lệ này được thực hiện thông qua xác thực mã hóa (cryptographic authentication).

# Giải pháp xác thực thư điện tử DKIM

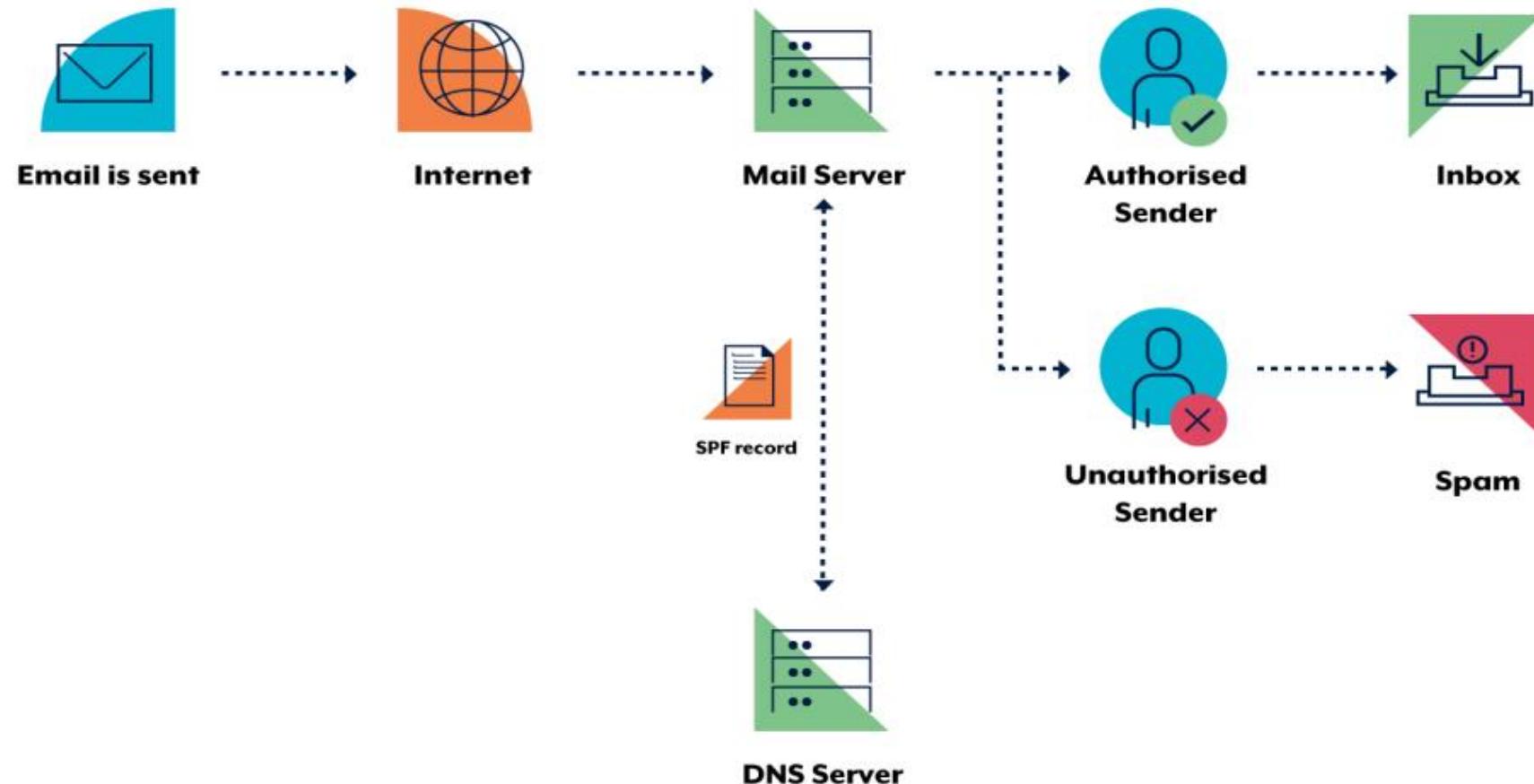
## ❖ Bên gửi email:

- Khi thực hiện gửi email, hệ thống thư điện tử (máy chủ Mail) của người gửi sẽ sinh ra cặp khóa private/public (có nhiều phần mềm hỗ trợ việc này ví dụ như OpenSSL,...) đối với một số máy chủ Mail thì có hỗ trợ việc tạo các khóa này.
- Khóa Public được thông báo công khai bằng cách khai báo trong bản ghi TXT trên hệ thống DNS theo đúng domain gửi email.
- Khóa Private còn lại được sử dụng để ký vào email trước khi gửi email. Khóa này chỉ lưu trên máy chủ Mail một cách an toàn nên không thể giả mạo.

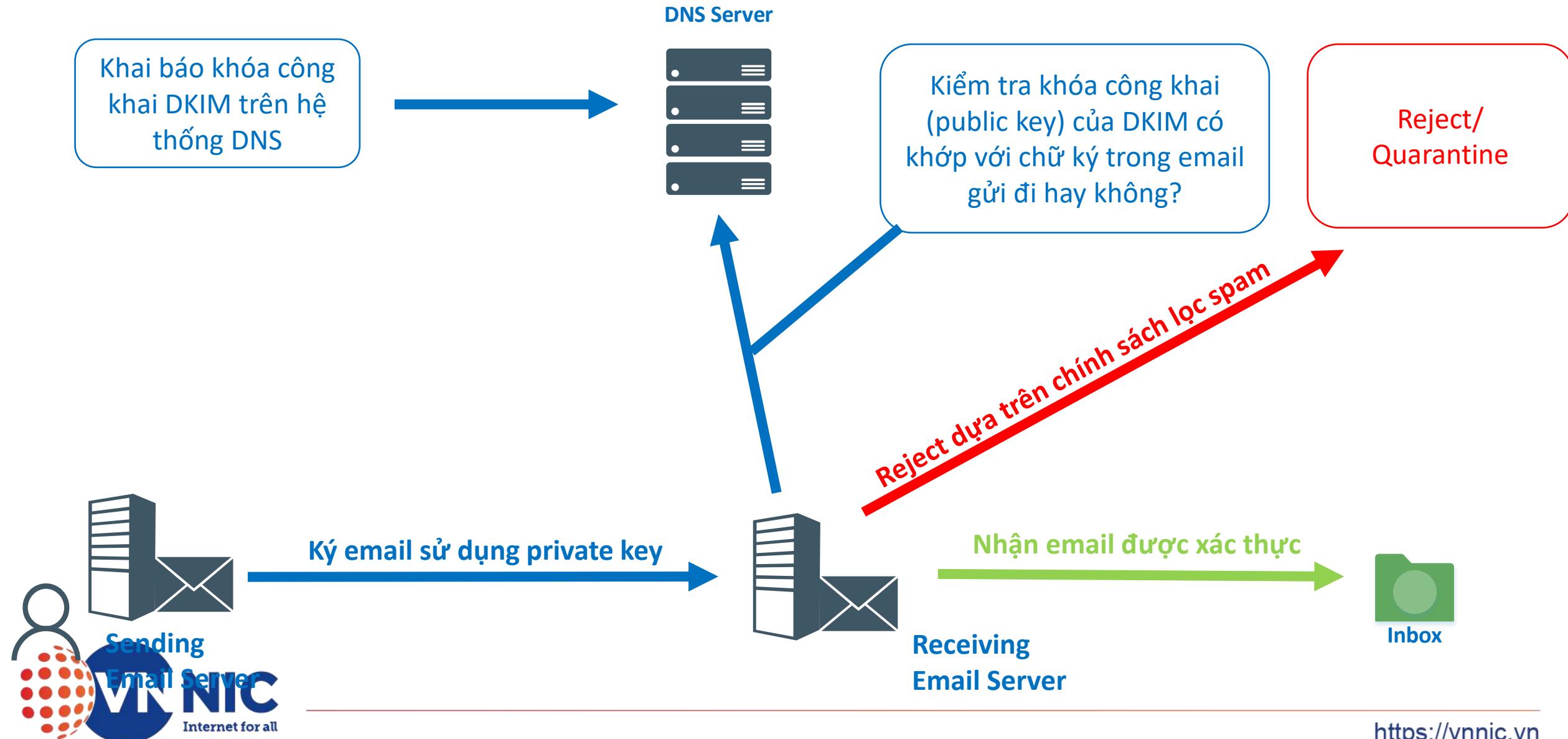
## ❖ Xử lý ở bên nhận:

- Nhận được email từ bên gửi và thấy email có thông điệp được mã hóa do cấu hình DKIM.
- Thực hiện truy vấn DNS để lấy khóa public của domain bên gửi để giải mã, nếu giả mã đúng thì xác nhận nguồn gửi và email đảm bảo, ngược lại sẽ tùy chỉnh sách của bên nhận để từ chối hoặc nhận email.

# Giải pháp xác thực thư điện tử SPF



# Giải pháp xác thực thư điện tử DKIM



# Giải pháp xác thực thư điện tử DKIM

**DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=ietf.org; s=ietf1; t=1432264097;  
bh=DnGEIxFloMduuUnbGf/ktbNUxOx7JkZRbjuQFmsr70M=; h=From:To:In-Reply-To:References:Date:Message-ID:MIME-  
Version:Cc:Subject: List-Id>List-Unsubscribe>List-Archive>List-Post:Content-Type:Sender;  
b=t6F/a3rYjOLKdEp8psEy2Afcljxx0ibZsfRGHsGA7L4xOuwS9aGAwI/XpxWOTcAY ...**

a=	Hashing algorithm used (SHA256)
b=	Signature data, a hash including the body hash and headers
bh=	Body hash, computed from the message body (up to l= bytes)
d=	Signing Domain Identifier (SDID)
h=	Headers included in signature
i=	Agent or User Identifier (AUID), optional
l=	Length limit of body included in body hash, optional
s=	Selector, identifies which public key to use to verify
t=	Time the signature was computed
x=	Expiration time of signature, optional

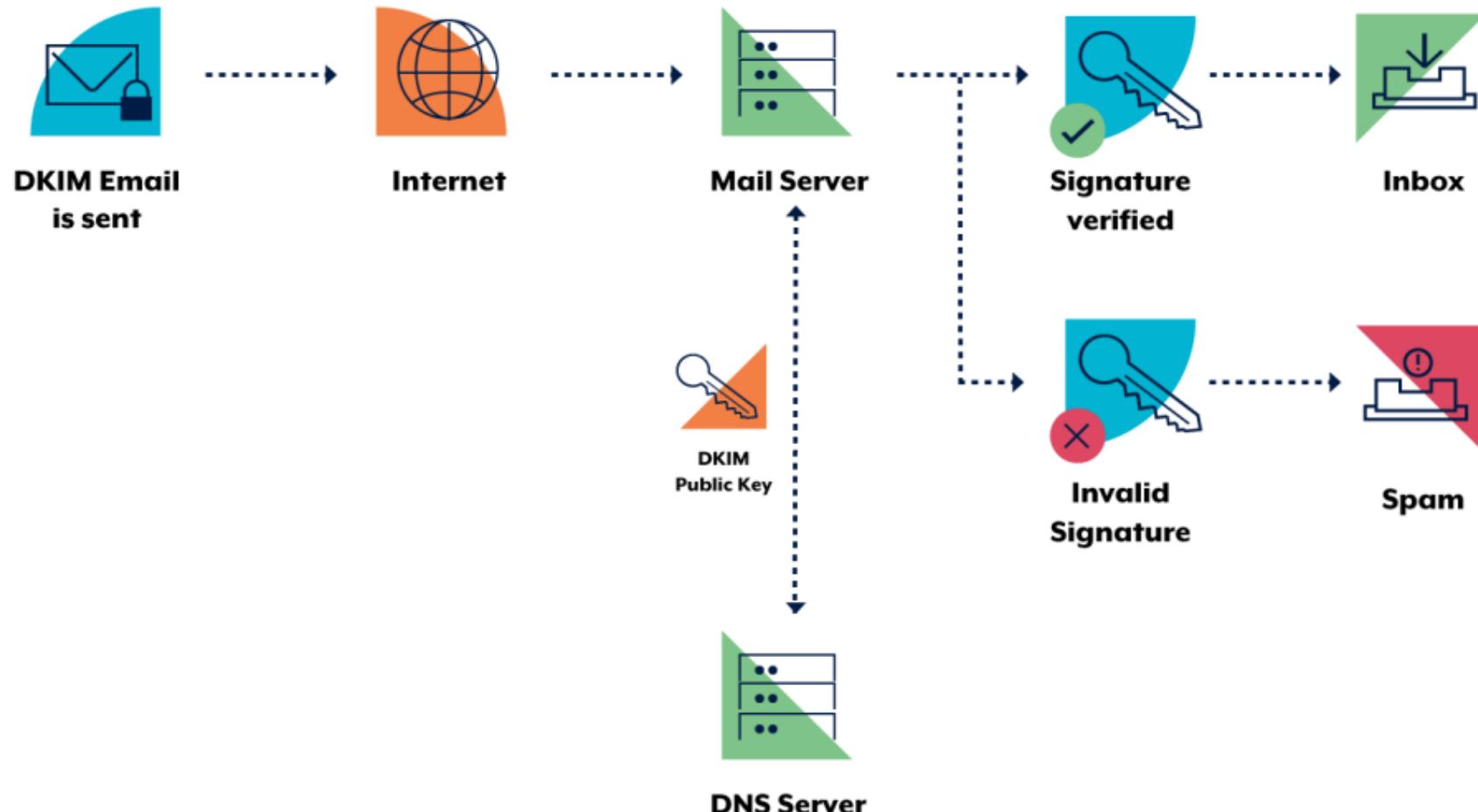
# Giải pháp xác thực thư điện tử DKIM

## ❖ Hạn chế

- SPF không hiệu quả trong việc chuyển tiếp (forwarding) và mailing list.
- DKIM không ký tất cả các phần của thư và chỉ ủy quyền một số phần, nên các tác nhân độc hại có thể chuyển tiếp email bằng cách thêm nhiều trường tiêu đề (header) vào đó. Chữ ký sẽ vẫn khớp với nó và vẫn được xác minh DKIM, do đó khiến người nhận thư được chuyển tiếp dễ bị tấn công.

# Giải pháp xác thực thư điện tử DKIM

## ❖ Mô hình triển khai



# Giải pháp xác thực thư điện tử DKIM

## ❖ Hướng dẫn triển khai:

- Quá trình xác thực thư điện tử bằng chữ ký DKIM sẽ được thực hiện trên các máy chủ Mail server (MTA) theo tên miền của đơn vị, tổ chức sở hữu tên miền.
  - ✓ Bước 1: Cài đặt và cấu hình DKIM trên máy chủ Mail server (MTA) của tên miền tương ứng được thực hiện xác thực bằng chữ ký DKIM.
  - ✓ Bước 2: Tạo cặp khóa Public key và Private key sử dụng cho DKIM.
  - ✓ Bước 3: Công khai khóa Public key bằng cách khai báo bản ghi DNS loạt TXT cho khóa Public key của DKIM trên hệ thống DNS hosting (hệ thống DNS quản lý tên miền của đơn vị, tổ chức).
  - ✓ Bước 4: Nâng cấp các máy chủ mail hoặc phần mềm hỗ trợ DKIM.

# Giải pháp xác thực thư điện tử DMARC

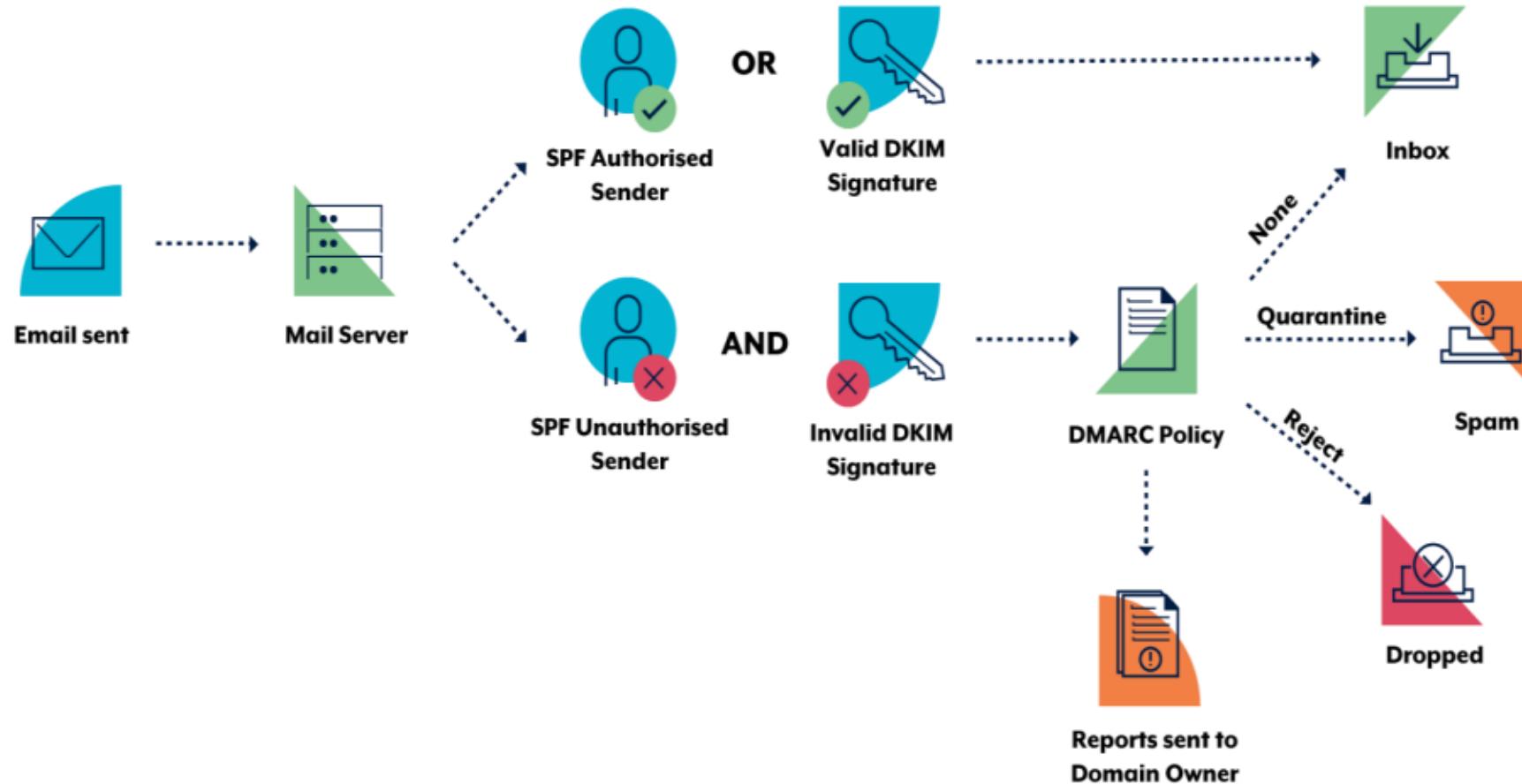
## ❖ Domain-based Message Authentication, Reporting and Conformance (DMARC).

- Là một phương pháp xác thực thư điện tử được thiết kế để phát hiện và ngăn chặn sự giả mạo thư điện tử.
- Được xây dựng dựa trên 2 giao thức đã được triển khai rộng rãi trước đó là SPF và DKIM. DMARC cho phép chủ sở hữu một tên miền công khai một chính sách về giao thức nào (DKIM hoặc SPF hoặc cả hai) được sử dụng khi gửi thư từ tên miền này và cách máy chủ nhận thư xử lý những trường hợp “fail”.
- DMARC cũng cung cấp một cơ chế báo cáo về những hoạt động được thực hiện dưới những chính sách này.

# Giải pháp xác thực thư điện tử DMARC

- ❖ DMARC sử dụng cả SPF và DKIM để xác thực email:
  - Chữ ký DKIM vẫn hoạt động bình thường ngay cả khi SPF bị lỗi
  - Hoặc SPF vẫn hoạt động tốt ngay cả khi DKIM chỉ được cài đặt tạm thời
- ❖ DMARC cho phép xác nhận chính sách để cách ly (Quarantine) hoặc chặn (Block) các thư không xác thực.
- ❖ DMARC thu thập và báo cáo nhiều dữ liệu
- ❖ Để có thể xác thực vượt qua DMARC thì DKIM hoặc SPF phải “pass”. Nhưng:
  - Phải thêm các yêu cầu bổ sung về kết quả kiểm tra của DKIM và SPF
  - Trường hợp DKIM hoặc SPF “pass” không phải lúc nào cũng đồng nghĩa với việc xác thực vượt qua DMARC.

# Giải pháp xác thực thư điện tử DMARC



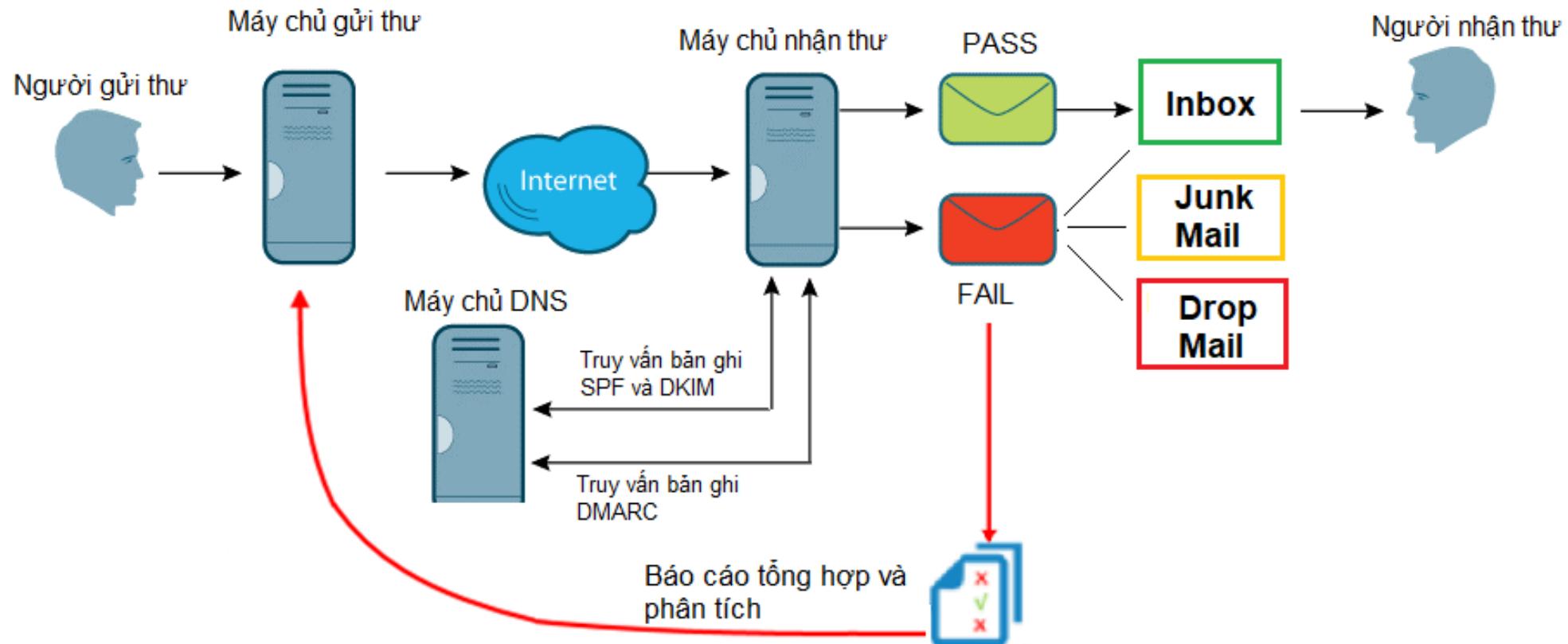
# Giải pháp xác thực thư điện tử DMARC

v=DMARC1; p=none; sp=quarantine; pct=100; ri=46,200; ruamailto:reports@dmarc.vn; rufmailto:reports@dmarc.vn

Field	Meaning	Default
v	Protocol version	DMARC1
p	Policy for the domain	none
sp	Policy for any subdomains	p= value
pct	% of messages to apply policy	100
adkim	DKIM alignment mode	r
aspf	SPF alignment mode	r
rua	Aggregate reporting URI(s)	
ruf	Failure reporting URI(s)	
rf	Failure report format	afrf
ri	Aggregate reporting interval	86400
fo	Failure reporting options	0

# Giải pháp xác thực thư điện tử DMARC

## ❖ Mô hình triển khai



# Giải pháp xác thực thư điện tử DMARC

## ❖ Hướng dẫn triển khai:

- Yêu cầu đầu tiên trước khi triển khai DMARC đó là tổ chức cũng đã triển khai SPF và/hoặc DKIM trước đó trên hệ thống thư điện tử của mình.
- Triển khai phương pháp xác thực thư điện tử bằng giao thức DMARC đơn giản chỉ bao gồm việc khai báo bản ghi DMARC (bản ghi DNS loại TXT) trên hệ thống DNS hosting tên miền được quản lý. Cụ thể, trên hệ thống DNS hosting tên miền này, thực hiện khai báo bản ghi DMARC sau:
- Ví dụ:

`_dmarc.test-mail.vnnic.vn. IN TXT "v=DMARC1; p=quarantine; fo=1;  
rua=mailto:rua@test-mail.vnnic.vn; ruf=mailto:ruf@test-mail.vnnic.vn; ri=3600;"`

# Giải pháp xác thực thư điện tử DMARC

## ❖ Hướng dẫn triển khai:

- Sau khi đã thực hiện khai báo thành công bản ghi DMARC trên hệ thống DNS hosting tên miền test-mail.vnnic.vn:
  - ✓ Tạo các hòm thư tương ứng với giá trị trong tag “rua=” và “ruf=” để nhận các báo cáo phân tích và tổng hợp gửi từ máy chủ nhận thư. Hai hòm thư tương ứng là: [rua@test-mail.vnnic.vn](mailto:rua@test-mail.vnnic.vn) và [ruf@test-mail.vnnic.vn](mailto:ruf@test-mail.vnnic.vn) như đã được khai báo trong bản ghi DMARC.

## Kết luận

- ❖ Việc triển khai đồng thời 3 giải pháp SPF, DKIM và DMARC sẽ giúp cho chúng ta hạn chế thấp những rủi ro phải đối mặt trong trường hợp giả mạo thư điện tử và hạn chế các vấn đề đối với thư rác gửi đến hệ thống. Trong đó:
  - SPF đóng vai trò chốt chặn đầu tiên, kiểm soát email và xác nhận từ người gửi hợp lệ.
  - DKIM sẽ là giải pháp trung tâm, đảm bảo khả năng xác thực và toàn vẹn dữ liệu của thư điện tử trong quá trình truyền tải.
  - DMARC sẽ dựa trên SPF & DKIM, để triển khai thêm các khả năng nhận dạng khác. Đảm bảo cho các thư điện tử được kiểm soát chính xác theo một chính sách xác định, đồng thời gửi lại các báo cáo thống kê quá trình xác thực email trên hệ thống.

# ❖ PHẦN 2: KHUYẾN NGHỊ HỆ THỐNG DNS CHO CÁC CQNN

## ❖ Phần 1: Hệ thống DNS

- ✓ Lý thuyết hệ thống DNS
- ✓ DNS hoạt động IPv6
- ✓ DNSSEC
- ✓ Xác thực thư điện tử dựa trên DNS

## ❖ Phần 2: Khuyến nghị hệ thống DNS cho các CQNN

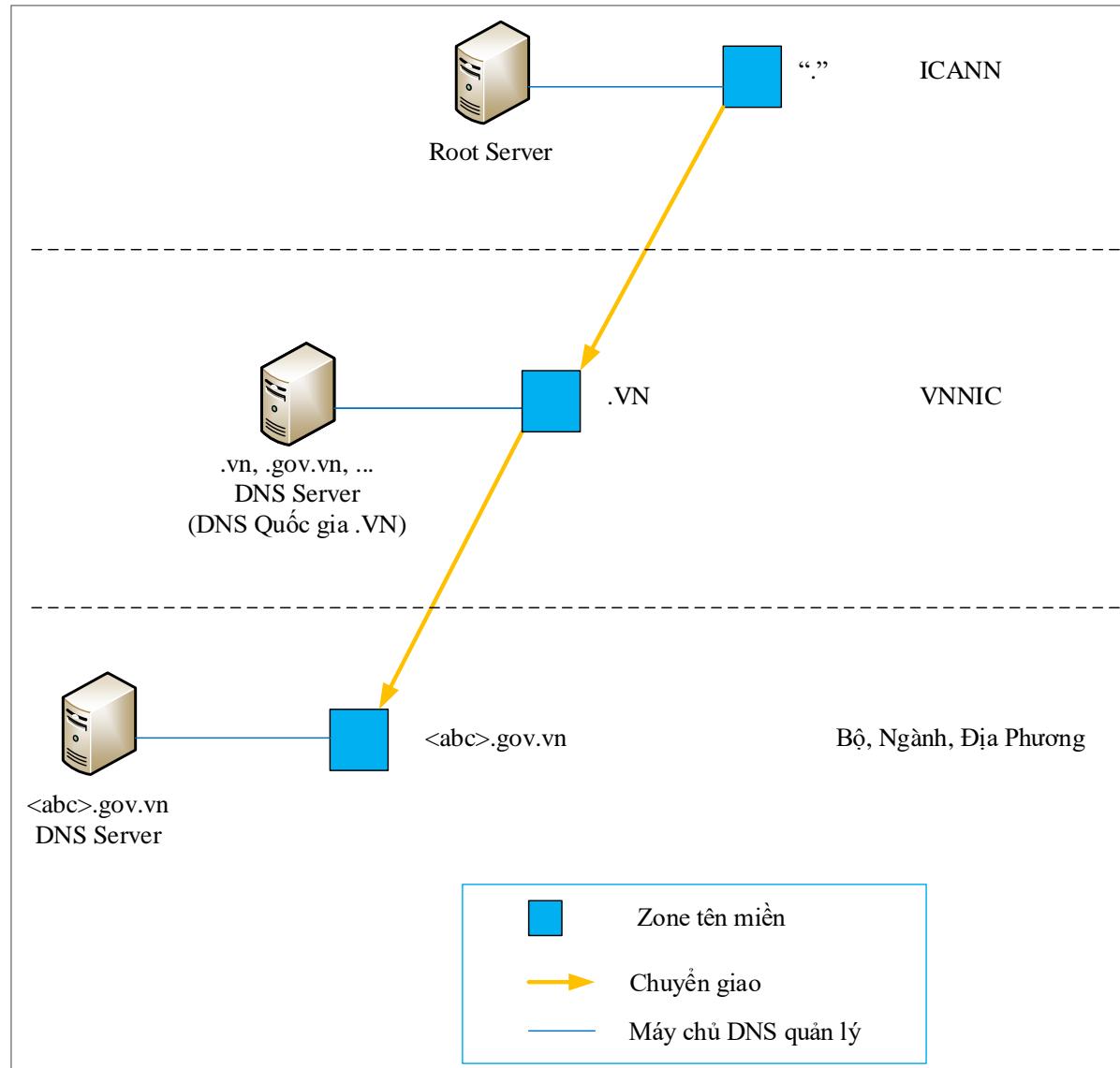
- ✓ **Khuyến nghị cho DNS Authoritative**
- ✓ **Khuyến nghị cho DNS Cache**
- ✓ **Xác thực thư điện tử Email Authentication**

## ❖ Phần 3: Thực hành DNS

- ✓ Cài đặt, cấu hình dịch vụ DNS
- ✓ Chuyển đổi IPv6 cho hệ thống DNS và Website
- ✓ Triển khai DNSSEC
- ✓ Xác thực thư điện tử Email Authentication

# 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/Nghành/Địa phương quản lý.
- ❖ Bộ/Nghành/Địa phương thiết lập hệ thống DNS để quản lý tên miền <ABC>.gov.vn được phân cấp.



# Hiện trạng hệ thống DNS của CQNN

- ❖ DNS quản lý tên miền <ABC>.gov.vn:
  - Đa số thuê DNS Hosting/một số có DNS riêng nhưng chưa quy chuẩn (mô hình thiếu dự phòng và đảm bảo an toàn, ...).
- ❖ DNS Cache:
  - Sử dụng các hệ thống Public DNS resolver: Google DNS, Cloudflare, ...



Google, Cloudflare, ...

Thuê ngoài/chưa chuẩn hóa

# Sự cần thiết cần có hệ thống DNS riêng

## ❖ DNS quản lý tên miền <ABC>.gov.vn:

- Các BNĐP đều có tên miền <ABC>.gov.vn đăng ký với Trung tâm Internet Việt Nam để triển khai các dịch vụ: email, cổng thông tin, dịch vụ công trực tuyến, 1 cửa điện tử, ...
- Các BNĐP cần có hệ thống máy chủ tên miền DNS để quản lý các tên miền của mình.

## ❖ DNS Cache:

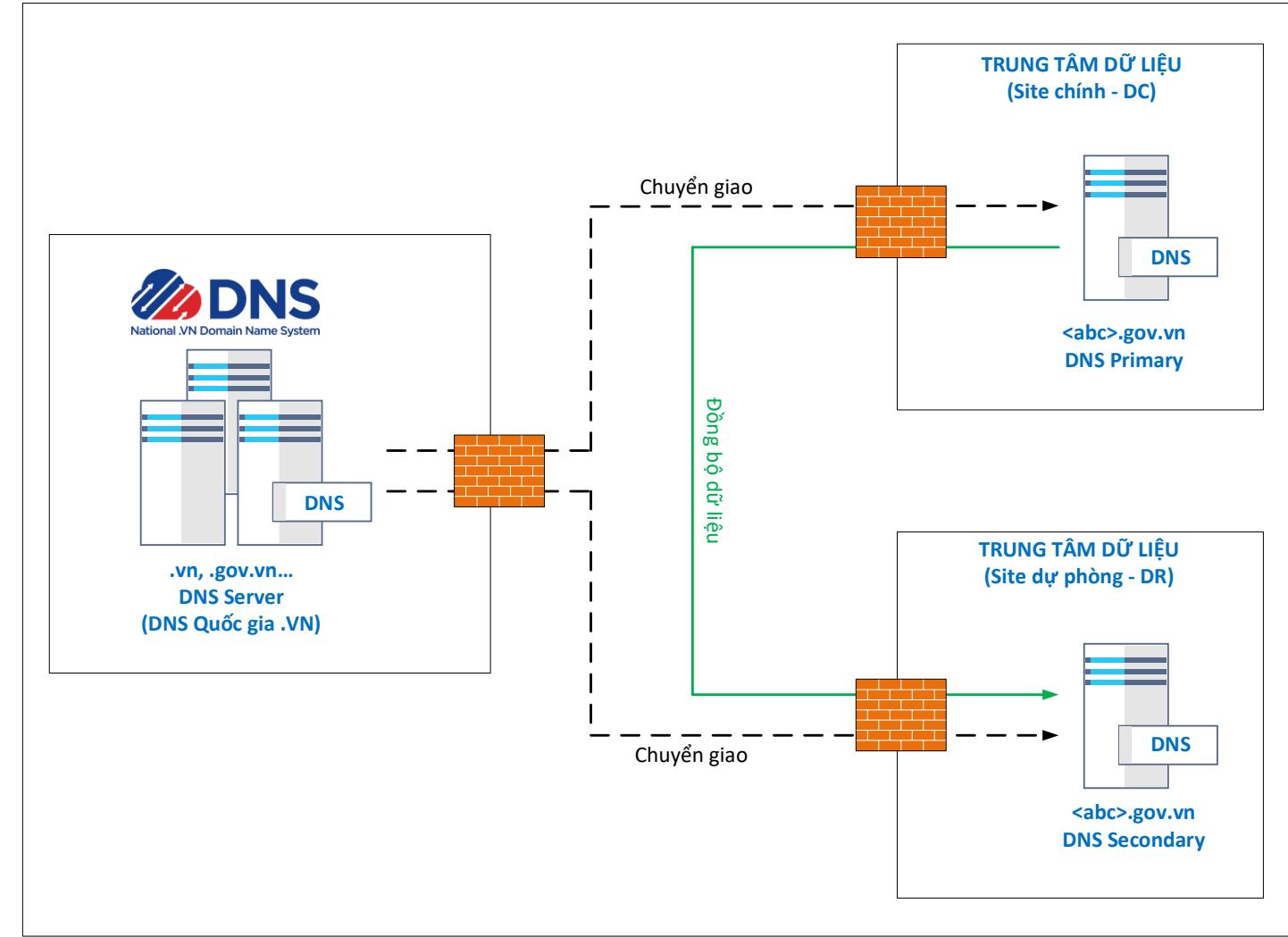
- Phục vụ truy cập các dịch vụ Internet sử dụng tên miền, truy vấn tên miền .VN và tên miền quốc tế của các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, ...) trong mạng của các đơn vị (BNĐP).
- Quản lý thiết lập chính sách truy cập tên miền tập trung, hệ thống DNS Cache có thể kết hợp với các hệ thống ATTT khác để bảo vệ chống mã độc, botnet.

## PHẦN 2: KHUYẾN NGHỊ HỆ THỐNG DNS CHO CÁC CQNN

### KHUYẾN NGHỊ DNS CACHE CHO CQNN

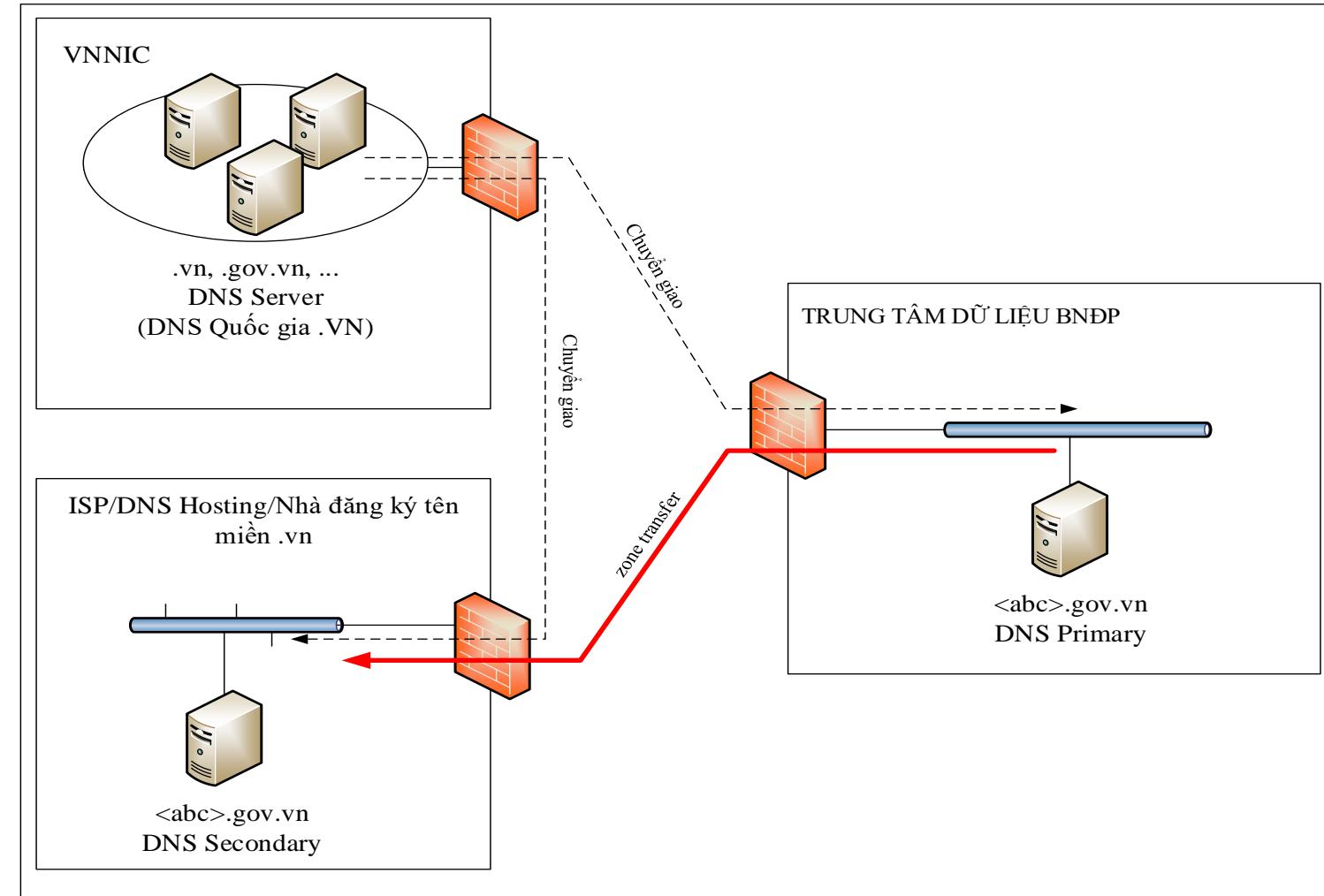
# Khuyến nghị DNS Authoritative cho CQNN

## ❖ Mô hình khuyến nghị



# Khuyến nghị DNS Authoritative cho CQNN

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



# Khuyến nghị DNS Authoritative cho CQNN

## ❖ Yêu cầu:

- 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 cho DNS Authoritative cho CQNN

## ❖ 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:

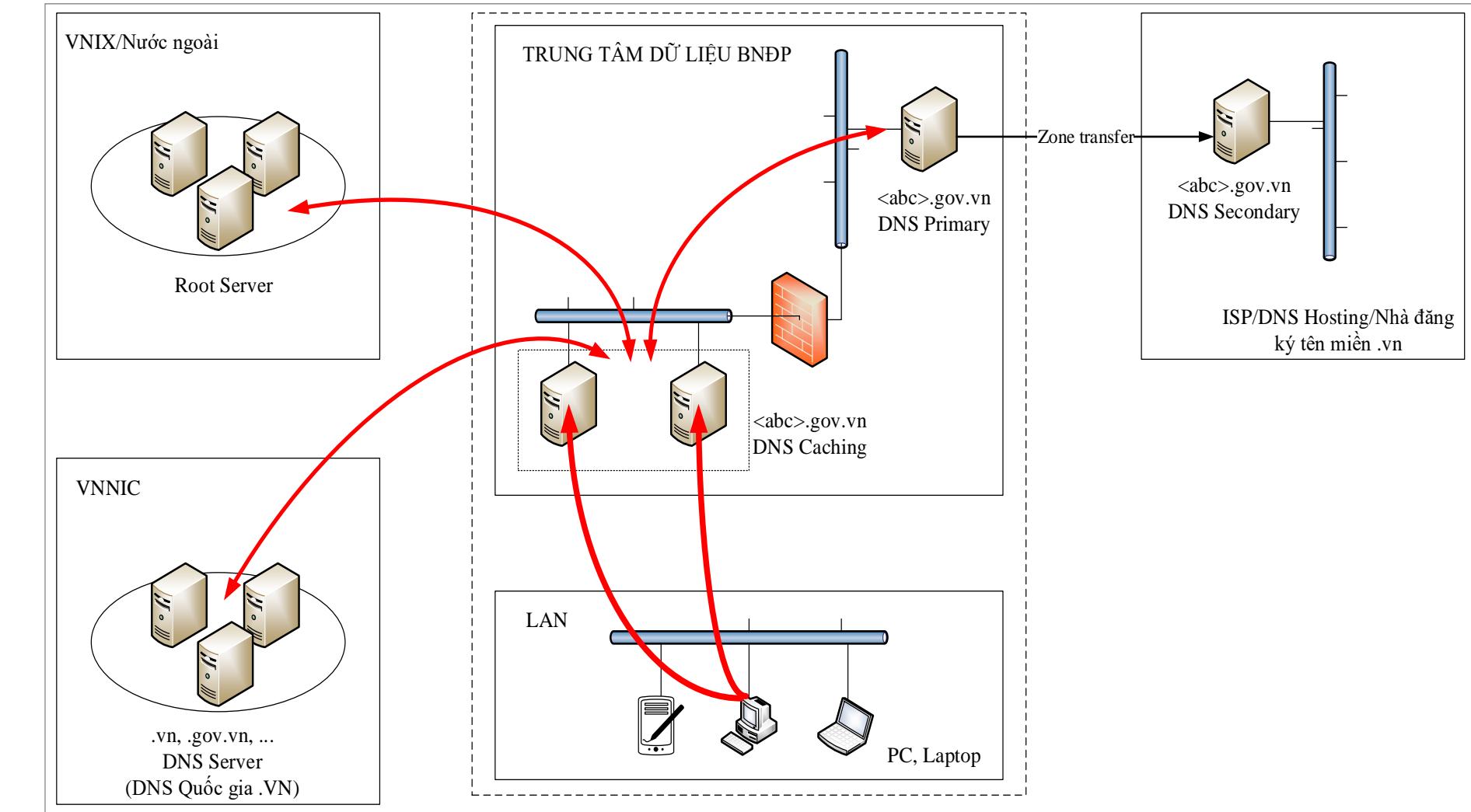
- Công văn số 273/BTTT-CBĐTW ngày 31/01/2020.
- Các tiêu chuẩn tham khảo: TCVN 11237-3:2015, TCVN 12044:2017; RFC1034, 1035, 1183, 1591, 3901, 4472, 4033, 4034, 4035, 4470, 4641, 5155, 6014.

## PHẦN 2: KHUYẾN NGHỊ HỆ THỐNG DNS CHO CÁC CQNN

### KHUYẾN NGHỊ DNS CACHE CHO CQNN

# Khuyến nghị DNS Cache cho CQNN

## ❖ Trích dẫn mô hình theo văn số 273/BTTT-CBĐTW



# Khuyến nghị cho DNS Cache cho CQNN

## ❖ Yêu cầu:

- 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 cho CQNN

## ❖ 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

## ❖ Tham khảo:

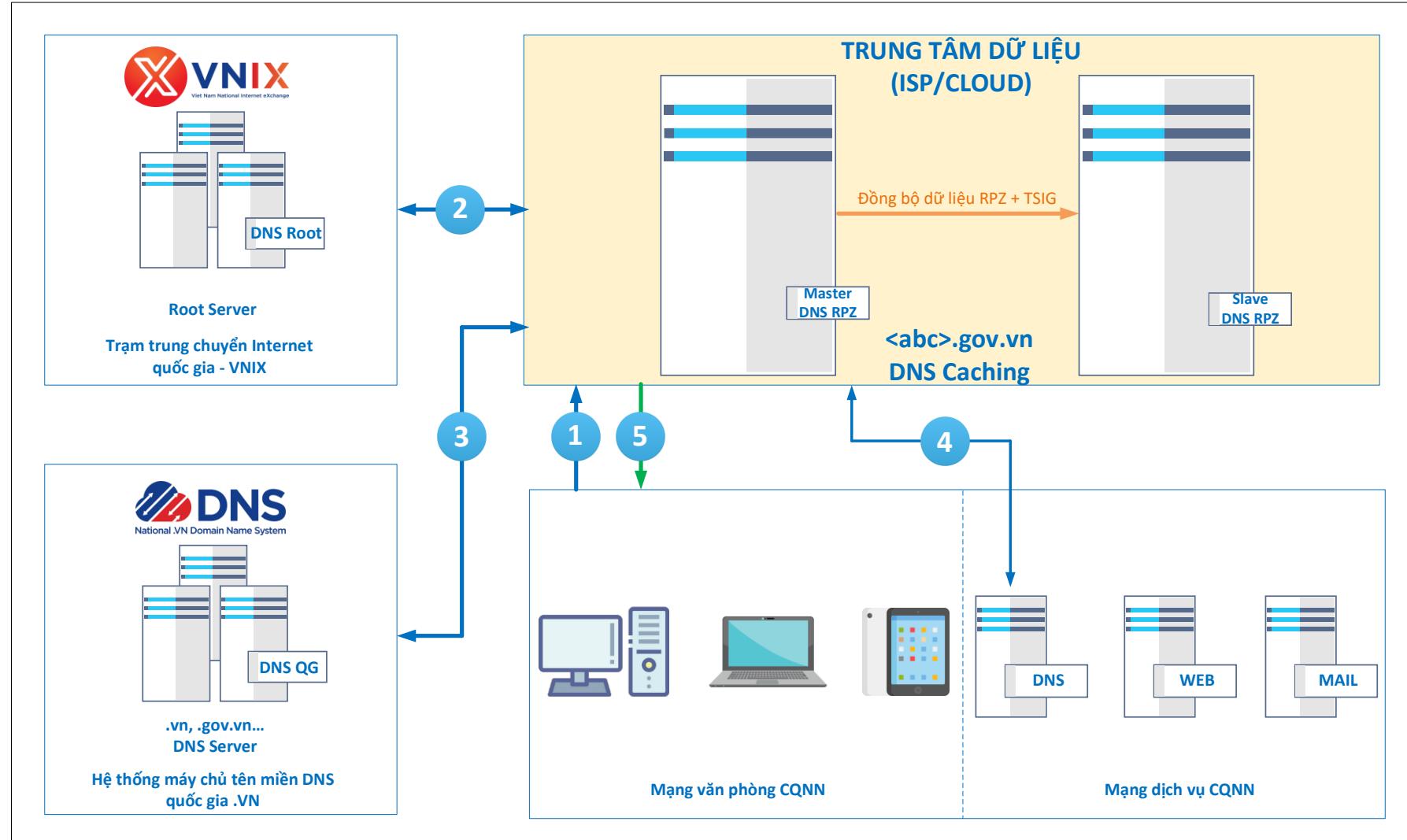
- Công văn số 273/BTTT-CBĐTW ngày 31/01/2020.
- Các tiêu chuẩn tham khảo: TCVN 11237-3:2015, TCVN 12044:2017; RFC1034, 1035, 1183, 1591, 3901, 4472, 4033, 4034, 4035, 4470, 4641, 5155, 6014.

## PHẦN 2: KHUYẾN NGHỊ HỆ THỐNG DNS CHO CÁC CQNN

### KHUYẾN NGHỊ DNS CACHE INTERNET SECURITY

# Khuyến nghị DNS Cache Internet Security

## ❖ Mô hình khuyến nghị



# Khuyến nghị DNS Cache Internet Security

## ❖ Khuyến nghị

- Triển khai DNS Cache thiết lập hoạt động RPZ như một Firewall mềm, dựa trên hoạt động của DNS để đảm bảo an toàn cho người dùng, dịch vụ và hệ thống của CQNN.
  - ✓ Triển khai 2 DNS Cache để đảm bảo tải và dự phòng
  - ✓ Sử dụng mô hình Master-Slave
  - ✓ Sử dụng TSIG

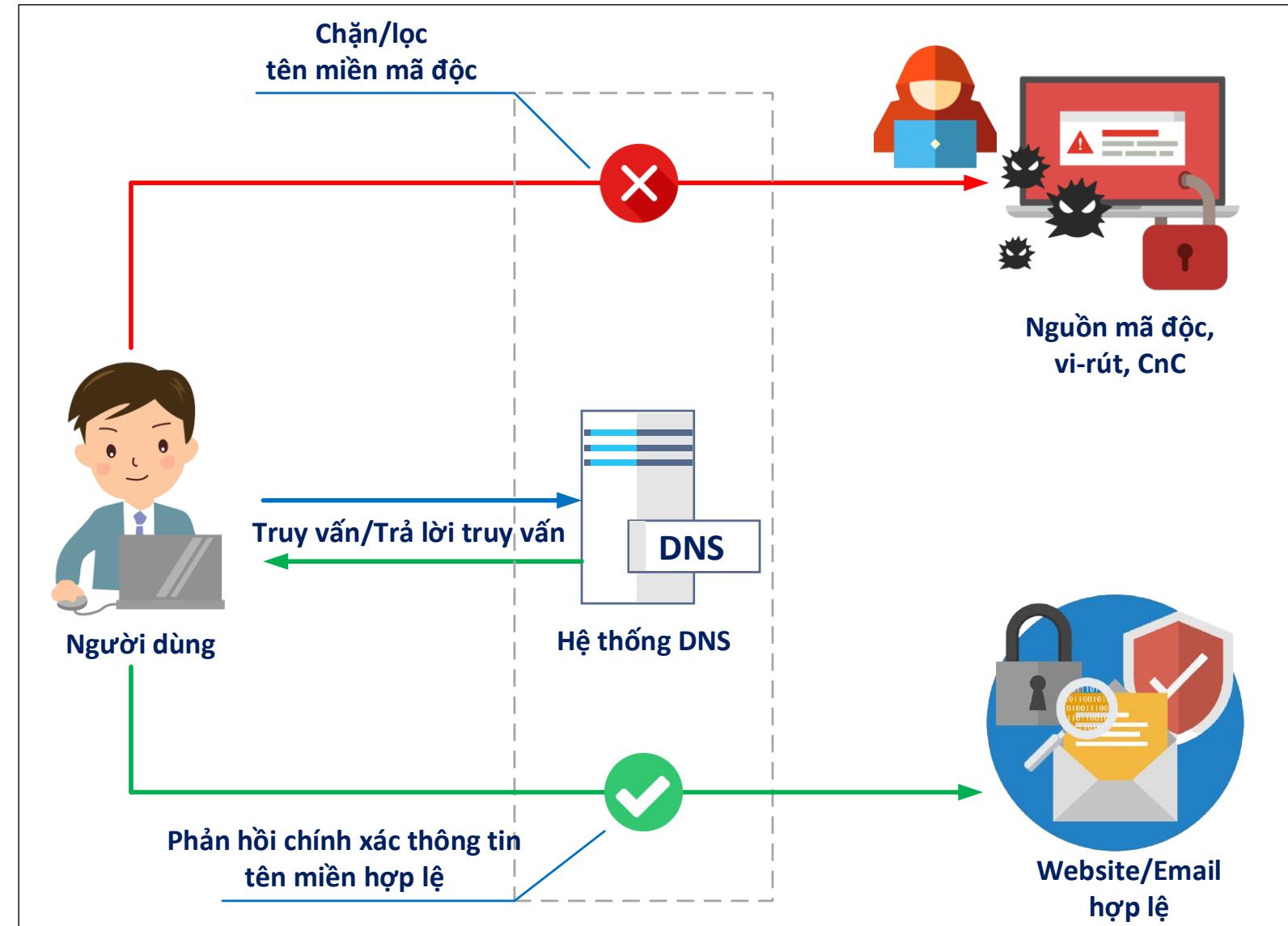
## ❖ Tham khảo

- ✓ Draft DNS Response Policy Zones (RPZ) <https://datatracker.ietf.org/doc/html/draft-vixie-dns-rpz-04>

## PHẦN 2: KHUYÊN NGHỊ HỆ THỐNG DNS CHO CÁC CQNN

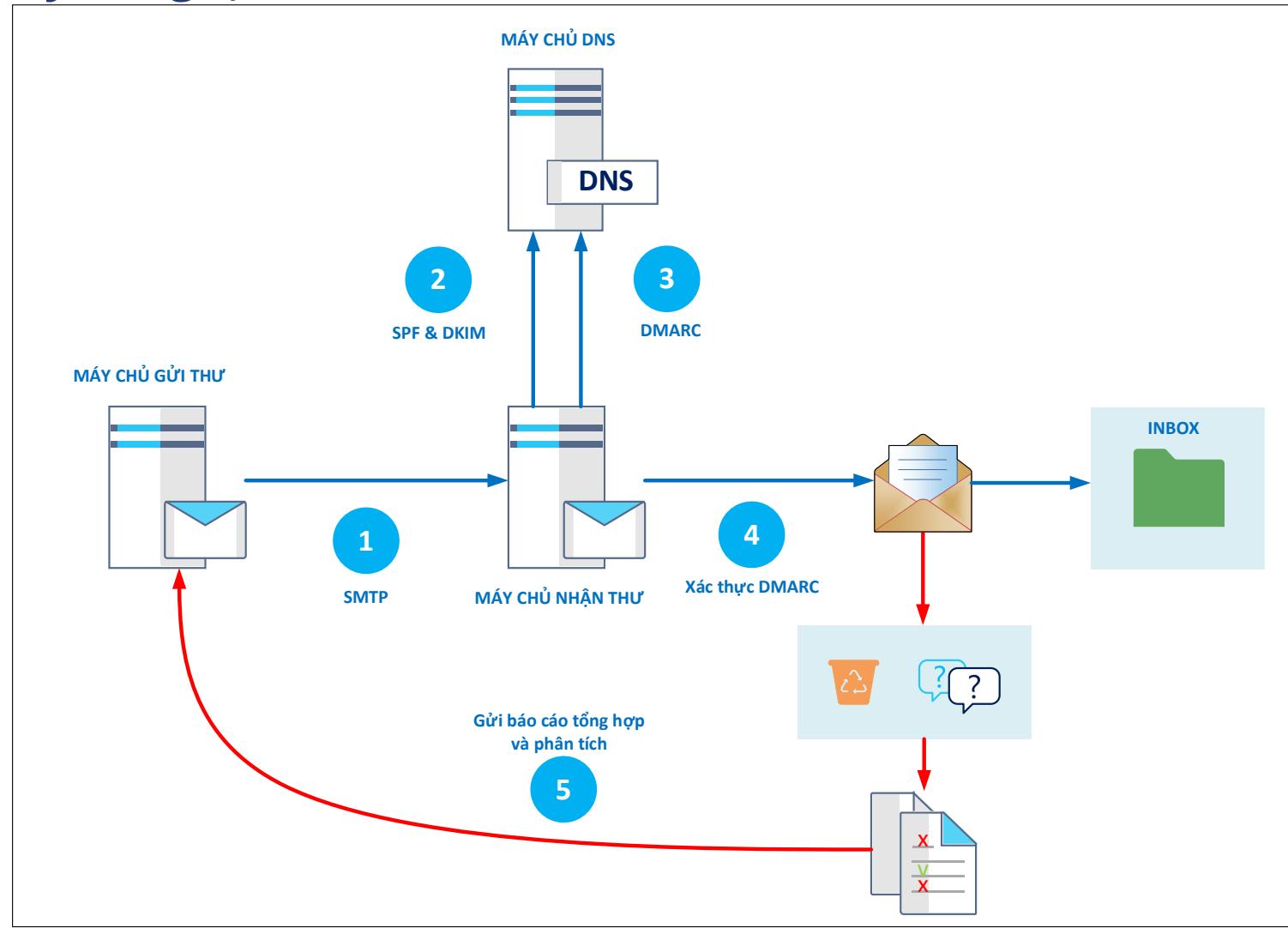
### XÁC THỰC THƯ ĐIỆN TỬ EMAIL AUTHENTICATION

# Xác thực thư điện tử Email Authentication



# Xác thực thư điện tử Email Authentication

## ❖ Mô hình khuyến nghị:



# PHẦN 3: THỰC HÀNH DNS

## ❖ Phần 1: Hệ thống DNS

- ✓ Lý thuyết hệ thống DNS
- ✓ DNS hoạt động IPv6
- ✓ DNSSEC
- ✓ Xác thực thư điện tử dựa trên DNS

## ❖ Phần 2: Khuyến nghị hệ thống DNS cho các CQNN

- ✓ Khuyến nghị cho DNS Authoritative
- ✓ Khuyến nghị cho DNS Cache
- ✓ Xác thực thư điện tử Email Authentication

## ❖ Phần 3: Thực hành DNS

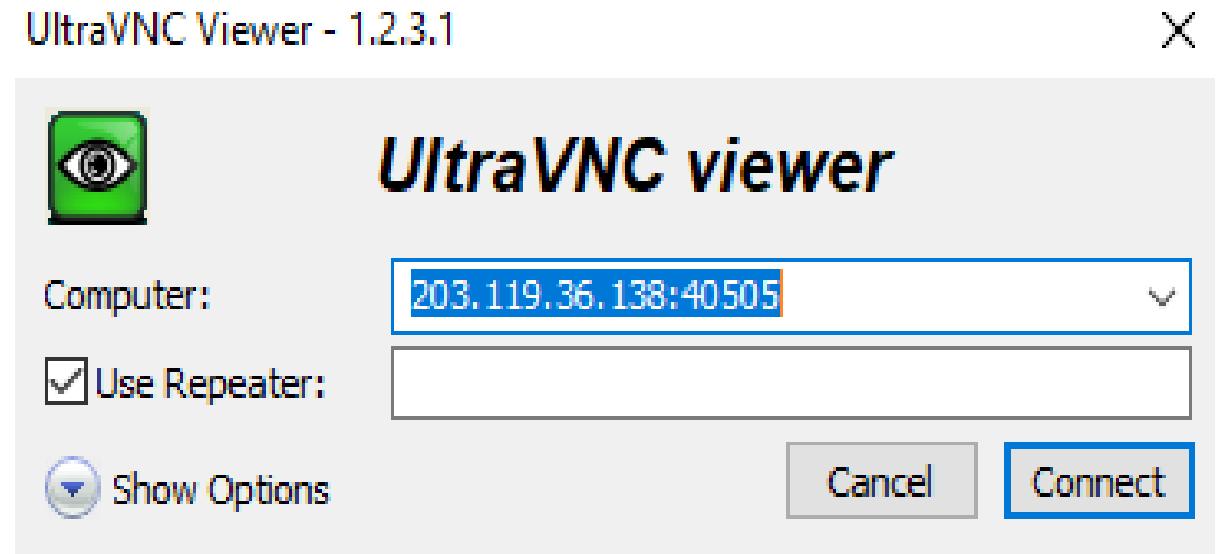
- ✓ Cài đặt, cấu hình dịch vụ DNS
- ✓ Chuyển đổi IPv6 cho hệ thống DNS và Website
- ✓ Triển khai DNSSEC
- ✓ Xác thực thư điện tử Email Authentication

# NỘI DUNG THỰC HÀNH DNS

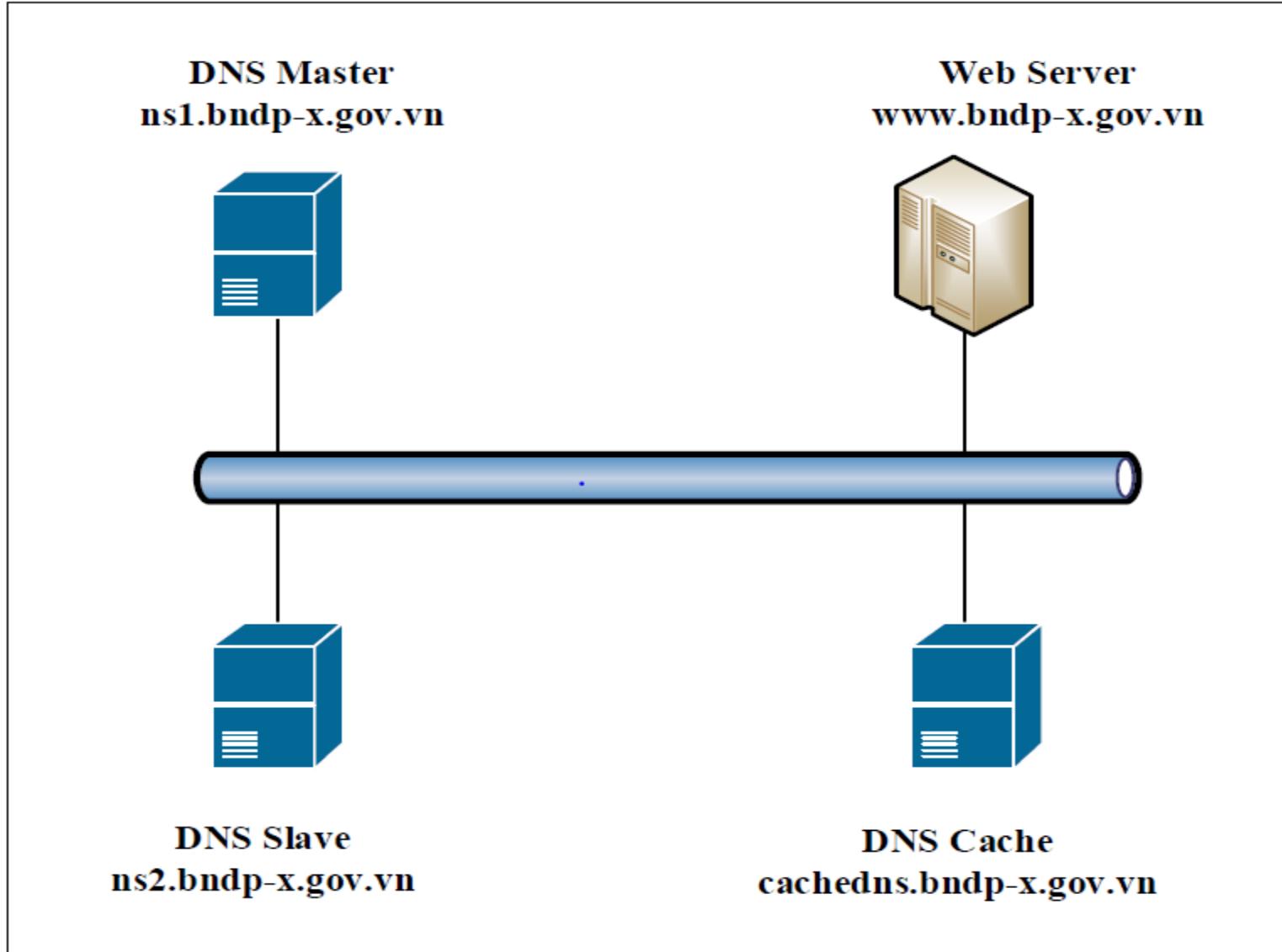
- ❖ Cài đặt, cấu hình dịch vụ DNS Authoritative
- ❖ Cài đặt, cấu hình dịch vụ DNS Cache
- ❖ Chuyển đổi IPv6 cho hệ thống DNS và Website
- ❖ Triển khai DNSSEC
- ❖ Xác thực thư điện tử Email Authentication

# NỘI DUNG CHUẨN BỊ

- Thực hiện truy cập vào trang web <https://www.eve-ng.net/index.php/download/> để thực hiện tải công cụ EVE-NG-Win-Client
- Thực hiện mở file và cài đặt EVE-NG-Win-Client
- Thực hiện mở UltraVNC View (đã cài đặt cùng với gói EVE-NG-Win-Client)
  - ✓ User: root
  - ✓ Password: \*\*\*\*\*



# MÔ HÌNH CÀI ĐẶT, CẤU HÌNH HỆ THỐNG DNS QUẢN LÝ TÊN MIỀN VÀ DNS CACHE





NÂNG TẦM THƯƠNG HIỆU VIỆT



## BỘ THÔNG TIN VÀ TRUYỀN THÔNG - TRUNG TÂM INTERNET VIỆT NAM

TP. Hà Nội: Tầng 24, Tòa nhà VNTA, Dương Đình Nghệ, Yên Hòa, Cầu Giấy, Hà Nội

TP. Đà Nẵng: Lô 21, Đường số 7, KCN An Đồn, Hải Châu, 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://facebook.com/myVNNIC/)

<https://vnnic.vn/>

Xin trân trọng  
cảm ơn !