# DNS TRONG LINUX

**Giảng viên hướng dẫn :** .....
**Sinh viên thực hiện** : LÊ THỊ THANH HIỀN
**Lớp** : S0809G
**MSSV** : .....

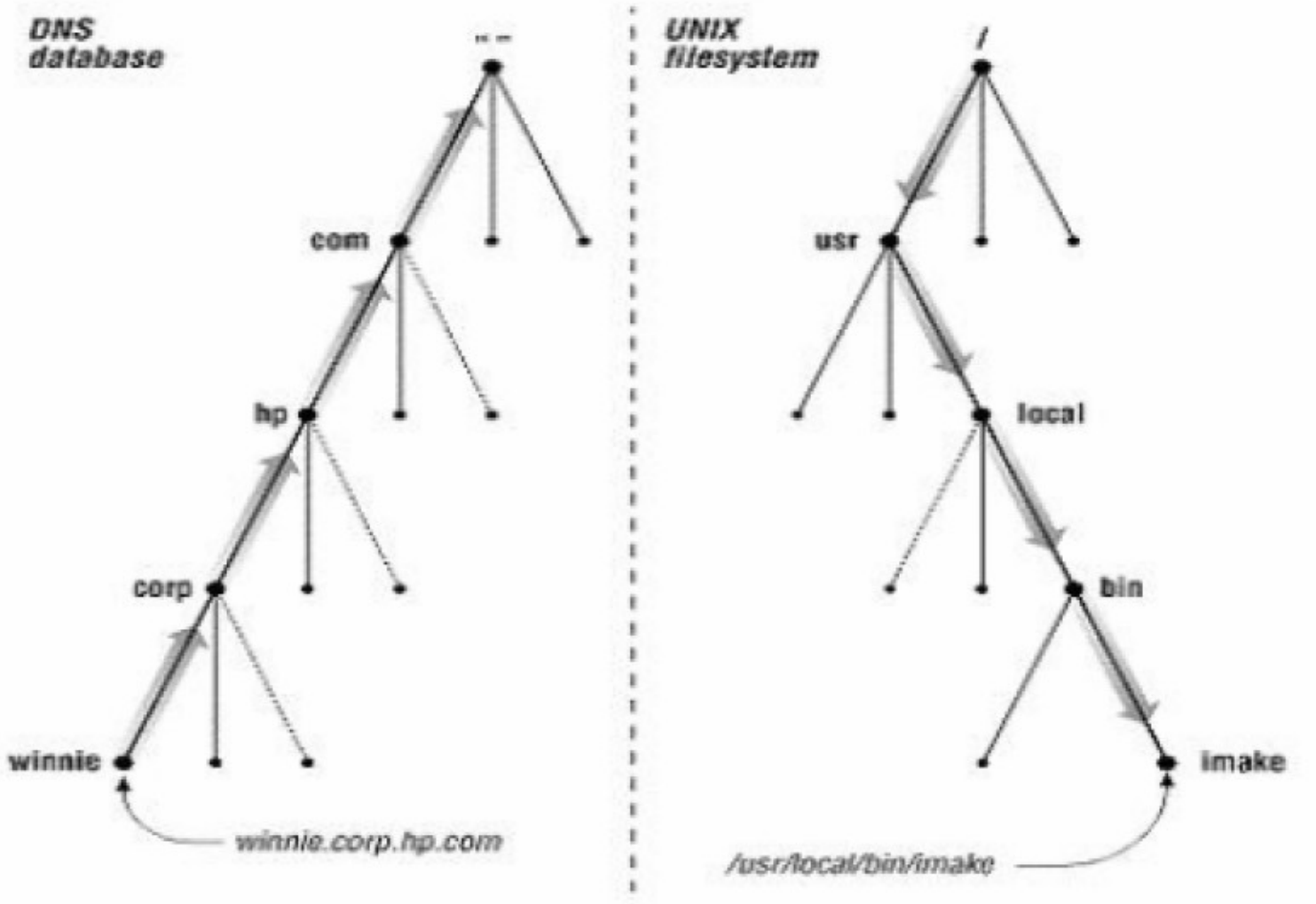
# DNS Trong Linux

- Giới thiệu về DNS
- Cơ chế phân giải
- Chứng nhận tên miền (FQDN)
- Phân loại Domain Name Server
- Sự ủy quyền
- Resource record
- Hoạt động của Name Server trong Linux
- Cấu hình

# 1. Giới thiệu về DNS

- Dịch vụ hoạt động theo mô hình Client-Server. Trong đó:
  - Server (name server): là máy chủ phục vụ tên.
  - Client (resolver): trình phân giải tên.
- DNS là một cơ sở dữ liệu phân tán.
- DNS được thi hành như một giao thức ở tầng Application trong mô hình TCP/IP.
- DNS phân bổ theo cơ chế phân cấp tương tự như sự phân cấp của hệ thống tập tin Unix/Linux.
- Cơ sở dữ liệu của DNS là một cây đảo ngược mỗi nút trên cây cũng là gốc của một cây con.

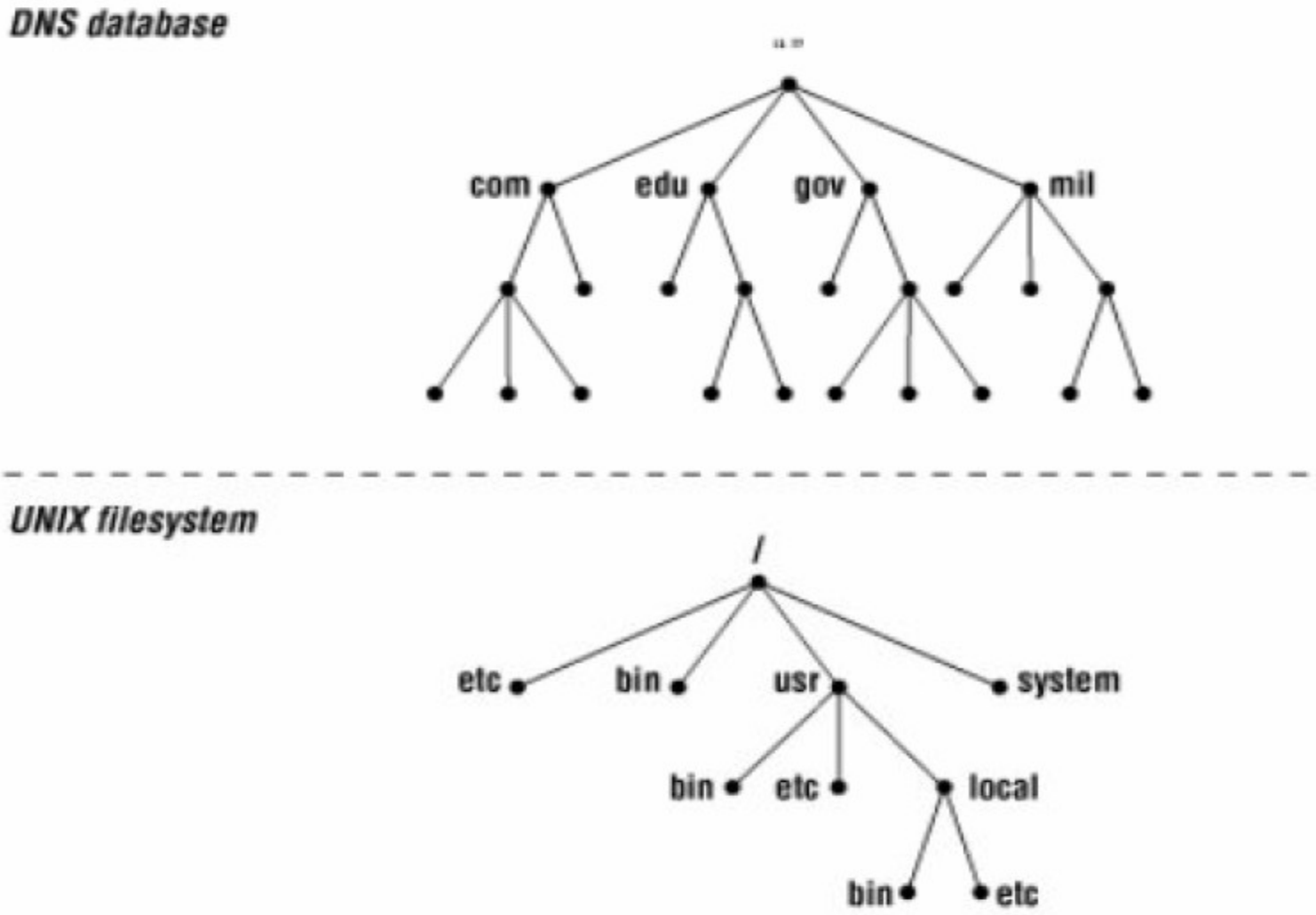
# 1. Giới thiệu về DNS



# 1. Giới thiệu về DNS

- Mỗi cây con là một phân vùng con trong toàn bộ CSDL DNS gọi là Domain.
- Mỗi Domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con Subdomain.

# 1. Giới thiệu về DNS



# 1. Giới thiệu về DNS

- Địa chỉ tên miền tổng quát:
  - host.subdomain.domain
- Trong đó:
  - host: tên máy.
  - subdomain: tên miền phụ.
  - Domain (top-level domain): tên miền chính.

# 1. Giới thiệu về DNS

# 1. Giới thiệu về DNS

- Cách phân bố dữ liệu quản lý domain name
  - Những root name server (.) quản lý những top-level domain trên internet. Tên máy và địa chỉ IP của những name server này được công bố cho mọi người biết.
  - Sơ đồ 13 root name server trên bản đồ thế giới.

# Vị trí 13 Root Name Server trên thế giới

# 2. Cơ chế phân giải

- Phân giải tên thành IP
  - Vai trò của Root name server: là máy chủ quản lý các name server ở mức top-level domain.
  - Khi có truy vấn về một tên miền nào đó thì root name server phải cung cấp tên và địa chỉ IP của name server quản lý top-level domain mà tên miền này thuộc vào.
  - Có hai loại truy vấn:
    - Truy vấn đệ quy
    - Truy vấn tương tác

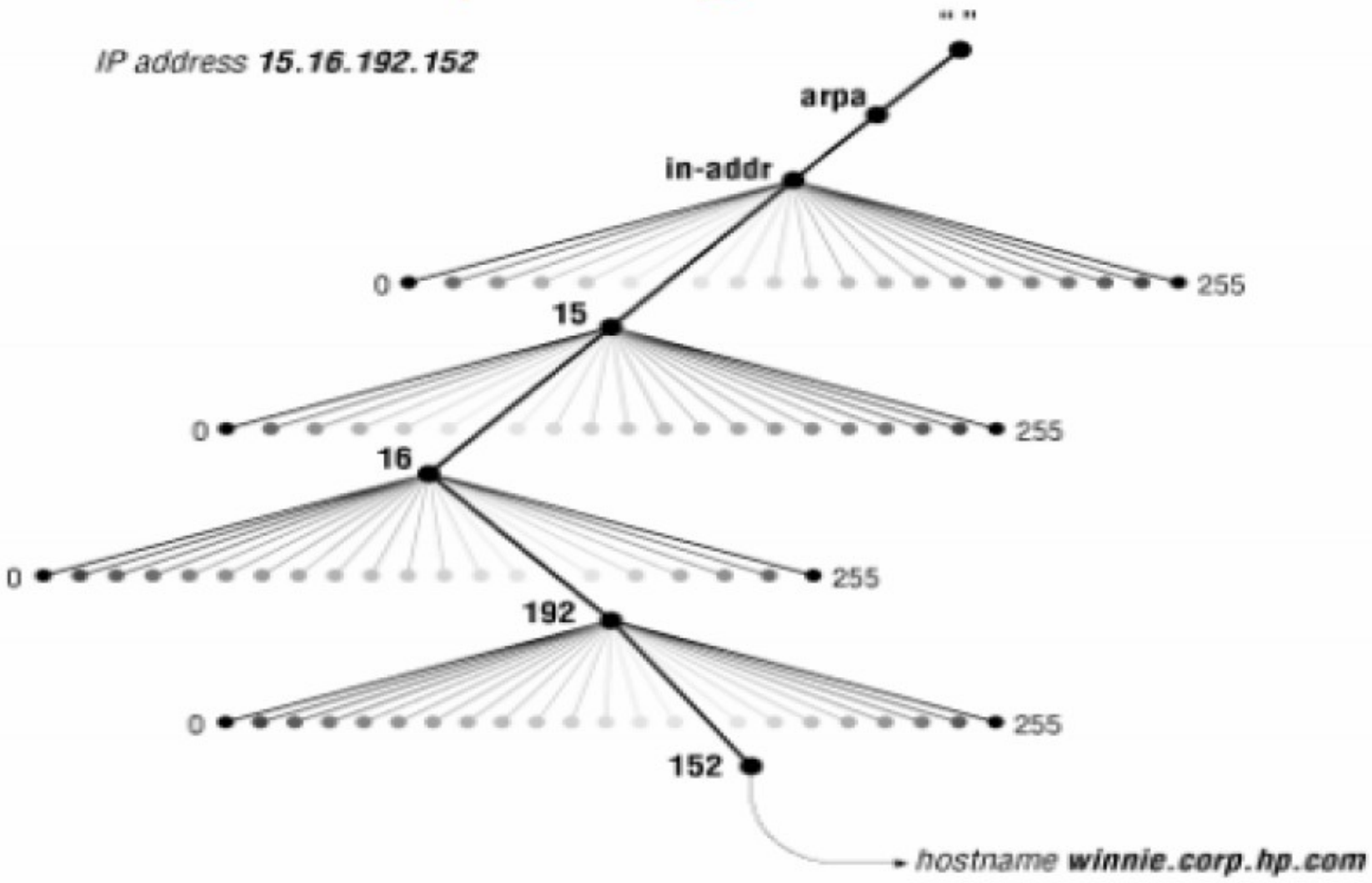
# 2. Cơ chế phân giải

- Phân giải IP thành tên máy tính

  Có thể phân giải tên máy tính thành một địa chỉ IP trong không gian tên miền người ta bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP. Phần không gian này có tên miền là:

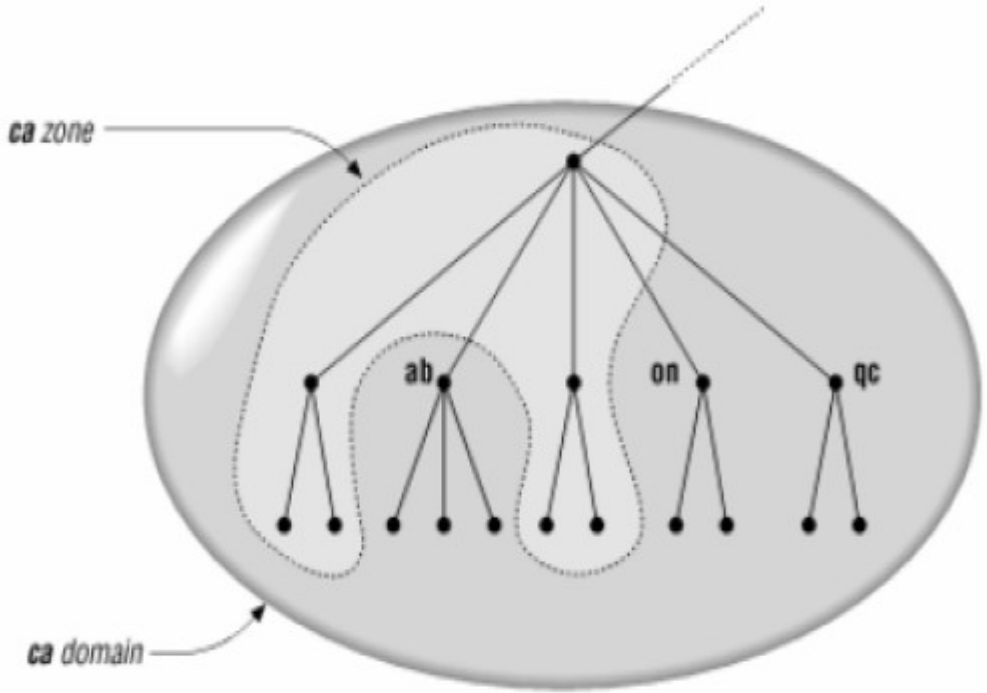
  .in-addr.arpa.

# 2. Cơ chế phân giải



# 2. Cơ chế phân giải

- Sự khác nhau giữa Domain Name và Zone
  - Zone: bao gồm một domain hay nhiều subdomain.
  - Domain Name: gồm nhiều submain và zone.



# Fully Qualified Domain Name (FQDN)

- Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiên tại đi ngược lên nút gốc, mỗi tên gọi cách ra bởi dấu chấm (.)
- Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (fully qualified  domain name FQDN)
- VD: https://vietnamnet.vn.

# 3. Phân loại Domain Name Server

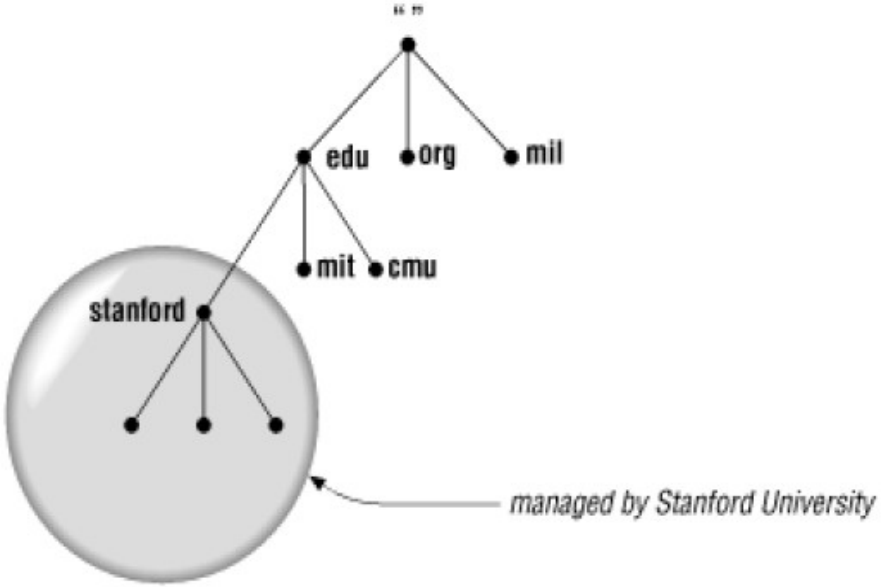
- Primary Name Server:
  - Mỗi miền phải có một Primary Name Server. Người quản trị DNS sẽ tốt chức những tập tin CSDL trên Primary Name Server. Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.
- Secondary Name Server
  - Sử dụng sao lưu tất cả những dữ liệu trân Primary Name Server và khi Primary Name Server bị gián đoạn thì nó sẽ đảm nhận phân giải tên máy thành địa chỉ IP và ngược lại.
  - Theo chu kỳ Secondary sẽ sao chép và cập nhật CSDL từ Primary Name Server, và tên và địa chỉ IP của Secondary Name Server cũng được mọi người trên Internet biết đến.

# 3. Phân loại Domain Name Server

- Caching Name Server
  - Có chức năng phân giải tên máy trên những mạng ở xa thông qua những Name Server khác. Nó lưu giữ những tên máy đã được phân giải trước đó và sử dụng:
    - Làm tăng tốc độ phân giải bằng cách sử dụng cache.
    - Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
    - Giảm việc lưu thông trên những mạng lớn.

# 4. Sự uỷ quyền

- Sự ủy quyền (Delegating Subdomains): Thông thường miền cha cung cấp các domain cho miền con dưới hình thức uỷ quyền cho miền con tự quản lý và tổ chức CSDL cho miền con.



# 5. Resource Record

- SOA (Start of Authority)
  - Trong mỗi zone file phải có một và chỉ có một SOA Record SOA chỉ ra rằng máy chủ name server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.
  - Cú pháp: [tên-miền] IN SOA [tên-server-dns] [địa chỉ email](
    - Serial number;
    - Refresh number;
    - Retry number;
    - Experi number;
    - Time – to – live number;)

# 5. Resource Record

- Serial:
  - Khi máy chủ secondary liên lạc với máy chủ Primary, trước tiên nó sẽ hỏi số serial, nếu số serial của máy chủ Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu zone trên Secondary đã cũ và sau đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có hiện hành.
  - Thông thường ta định dạng theo thời gian như sau: YYYYDDMM
  - Ví dụ: 2004122901

# 5. Resource Record

- ***Refresh***: chỉ ra khoảng thời gian máy chủ Secondary kiểm tra dữ liệu zone trên máy chủ Primary để cập nhật nếu cần.
  - Ví dụ: 10800; refresh sau 3 giờ.
- ***Retry***: nếu máy chủ Secondary không kết nối được máy chủ Primary theo thời gian mô tả trong refresh thì nó phải tìm cách kết nối lại với máy chủ Primary theo một chu kỳ thời gian mô tả trong rẻty. Thường giá trị này nhỏ hơn refresh.
  - Ví dụ: 3600; Retry sau 1 giờ.

# 5. Resource Record

- ***Experi***: nếu trong khoảng thời gian này máy chủ Secondary không kết nối được với máy chủ Primary thì máy chủ Secondary sẽ không trả lời cho vùng dữ liệu đó khi được truy vấn, vì nó cho rằng dữ liệu này đã quá cũ. Giá trị này phải lớn hơn giá trị refresh và retry.
  - Ví dụ: 604800; Experi sau 1 tuần

# 5. Resource Record

- ***Time-to-live***: giá trị được dùng cho tất cả các resource record trong file cớ sở dữ liệu. Giá trị này cho phép những server khác cache lại dữ liệu trong một khoảng thời gian xác định TTL.
  - Ví dụ: 86400; TTL là 1 ngày
- NS (Name Server)
  - Record tiếp theo cần có trong zone là NS record. Mỗi name server cho zone sẽ có một NS record.
  - Cú pháp: [tên-domain] IN NS [máy-DNS-Server]
    - Ví dụ: movie.edu. IN NS terminator.movie.edu

# 5. Resource Record

- Record A:
  - Ánh xạ tên vào địa chỉ
  - Cú pháp: [tên máy] IN A [địa chỉ IP]
  - Ví dụ: terninator.movie.edu. IN A 192.168.11.100
- Record CNAME:
  - Tạo tên bí danh alias trỏ vào một tên canonical. Tên canonical là tên host trong record A hoặc lại trỏ vào tên canonical khác.
  - Cú pháp: [tên máy alias] IN CNAME [tên máy gốc]
    - Ví dụ: server.movie.edu. IN CNAME terminator.movie.edu

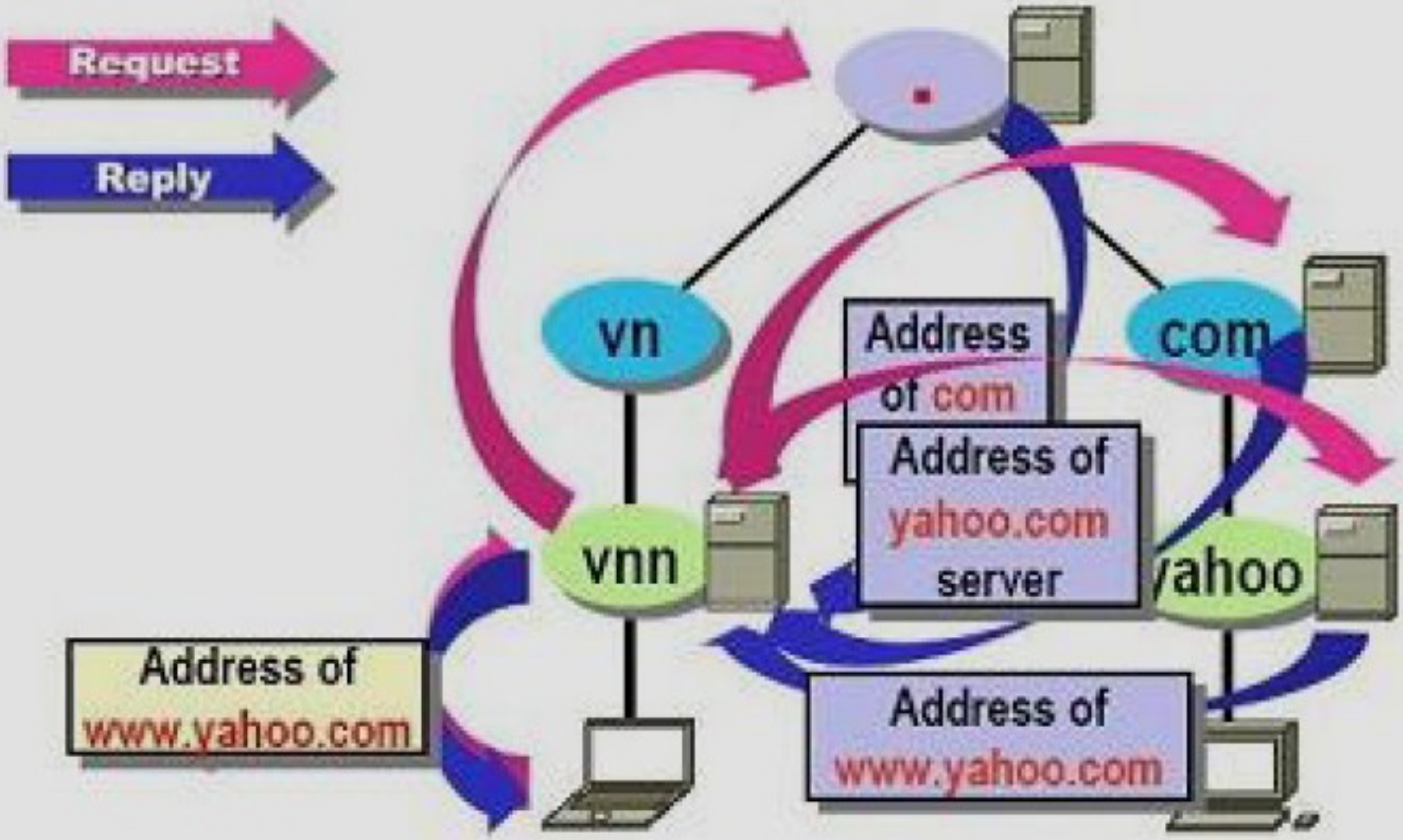
# 5. Resource Record

- MX (Mail Exchange)
  - DNS dùng record MX để thực hiện chuyển mail trên mạng internet.
  - Cú pháp: [tên-domain] IN MX [độ ưu tiên] [tên mail server]
  - Ví dụ: t3h.com IN MX 0 mail.t3h. Com
- PTR (Pointer):
  - Dùng để ánh xạ địa chỉ IP thành hostname.
  - Cú pháp: [địa chỉ IP] IN PTR [tên máy]
  - Vì dụ: 1.14.29.172.in-addr. arpa IN PTR server.t3h.com

# 6. Hoạt động của Name Server trong Linux

- Tất cả các DNS server được kết nối một cách logic với nhau:
  - Tất cả các DNS server đều được cấu hình để biết ít nhất một cách đến root server.
  - Một máy tính kết nối vào mạng phải biết làm thế nào để liên lạc với ít nhất là một DNS server.

# 6. Hoạt động của Name Server trong Linux



# 6. Hoạt động của Name Server trong Linux

- Khi có truy vấn DNS thì client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó.
- DNS server cũng có thể sử dụng thông tin trong cache hoặc nó có thể hỏi DNS server khác.

# 6. Hoạt động của Name Server trong Linux

- Trong Linux chương trình quản lý domain name gọi là BIND (Berkely Internet Name Domain)
- Chương trình server của DNS name server là một chương trình Daemon (named).
- Trong quá trình khởi động named đọc các tập dữ liệu rồi chờ các yêu cầu phân giải qua cổng xác định trong tập tin /ect/services.

# 6. Hoạt động của Name Server trong Linux

- Khi nhận được một yêu cầu từ resolver, đầu tiên named dùng giao thức UDP để truy vấn. Nếu giao thức này không có kết quả thì named dùng giao thức TCP/IP.
- Truy vấn từ Client đến Server sử dụng cổng nguồn là lớn hơn 1023, cổng đích là 53.
- Server trả lời truy vấn cho sử dụng cổng nguồn 53, cổng đích là lớn hơn 1023.
- Một truy vấn và trả lời server-to-server: với giao thức UDP port nguồn và đích đều là 53, với TCP truy vấn của server sẽ sử dụng port > 1023.

# 8. Cấu hình

- Cấu hình tập tin named.conf
  - Options: Định nghĩa những cấu hình toàn cục cho Bin

options {

Directory “thư_mục_chứa_csdl”; mặc định là thư mục /var/named

}

  - Zone: Định nghĩa một zone để quản lý CSDL cho miền hay miền con.
  - zone “tên_miền” {

# 8. Cấu hình

- Tập tin cấu hình named.conf
  - Zone: Định nghĩa một zone để quản lý CSDL cho miền hay miền con.

    zone “tên_miền” {

    type master/slave/hint/stub;

    masters {Đ/c IP của Primary Name server; }’

    file “tên_file_CSDL”;  };

    - type: + Master: server có bản copy chính csdl.

      + salve: lưu bản sao csdl từ master.

      + stub: tương tự như slave chỉ cho phép record NS từ Master

      + hint: zone chỉ ra những root name server.

# 8. Cấu hình

- Cấu hình Primary name server
  - Tạo tập tin named.conf
  - Thêm vào 2 zone:

```
zone “domain_name" {
        type master;
        file "named.localhost";
};
zone “domain ngược" {
        type master;
        file "named.loopback";
};
```

Ví dụ

```
zone “diendanspkt.net" {
        type master;
        file “diendanspkt.localhost";
};
zone “11.168.192.in-addr.arpa" {
        type master;
        file “diendanspkt.loopback";
};
```

# 8. Cấu hình

- Ví dụ: Tập tin named.conf

  /var/named/chroot/etc/named.conf

```
zone “test.com” IN {
    type master;
    file “test.com”;
};
zone “5.168.192.in-addr.arpa.” IN {
    type master;
    file “192.168.5.db”;
};
```

# 8. Cấu hình

- Cấu hình cho Secondary name server:
  - Chức năng của Secondary Name Server là backup dữ liệu từ Primary Name Server.
  - Không cần tạo các tập tin CSDL.
  - Chỉ khai báo 2 zone trong tập tin cấu hình như sau:

Zone “tên_miền” {

Type slave;

Masters {Đ/c IP của Primary Name server; }

File “tên_file_CSDL”; }

Khởi động lại named

# 8. Cấu hình

- Tạo tập tin named.conf
  - Thêm vào 2 zone: Ví dụ

```
zone “domain name" {
 type slave;
 masters {IP Primary NS;};
 file "named2.localhost";
};

zone “domain ngược" {
 type slave;
 masters {IP Primary NS;};
 file "named2.loopback";
};
```

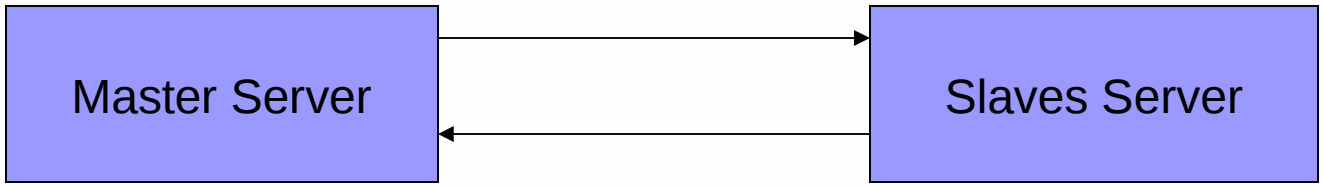
```
zone “net.com" {
        type slave;
        masters {192.168.11.1;};
        file "named2.localhost";
};

zone “11.168.192.in-addr.arpa" {
        type slave;
        masters {192.168.11.1;};
        file "named2.loopback";
};
```

# 8. Cấu hình

- Cấu hình DNS Client:
  - Cấu hình DNS client nhằm sử dụng công cụ nslookup để kiểm tra những Name Server vừa được cấu hình.
  - Trong Linux, những thông số cấu hình DNS Client được lưu trong tập tin /etc/resolv.conf.
- Nội dung tâp tin này:
  - nameserver <địa chỉ IP của Name-Server>
  - domain <tên miền>
- Ví dụ
  - Nameserver 172.29.50.1; Domain net01.com

# Cấu hình

- Cấu hình DNS master server và DNS slave Server.




•Cấu hình DNS master – slave , cha con