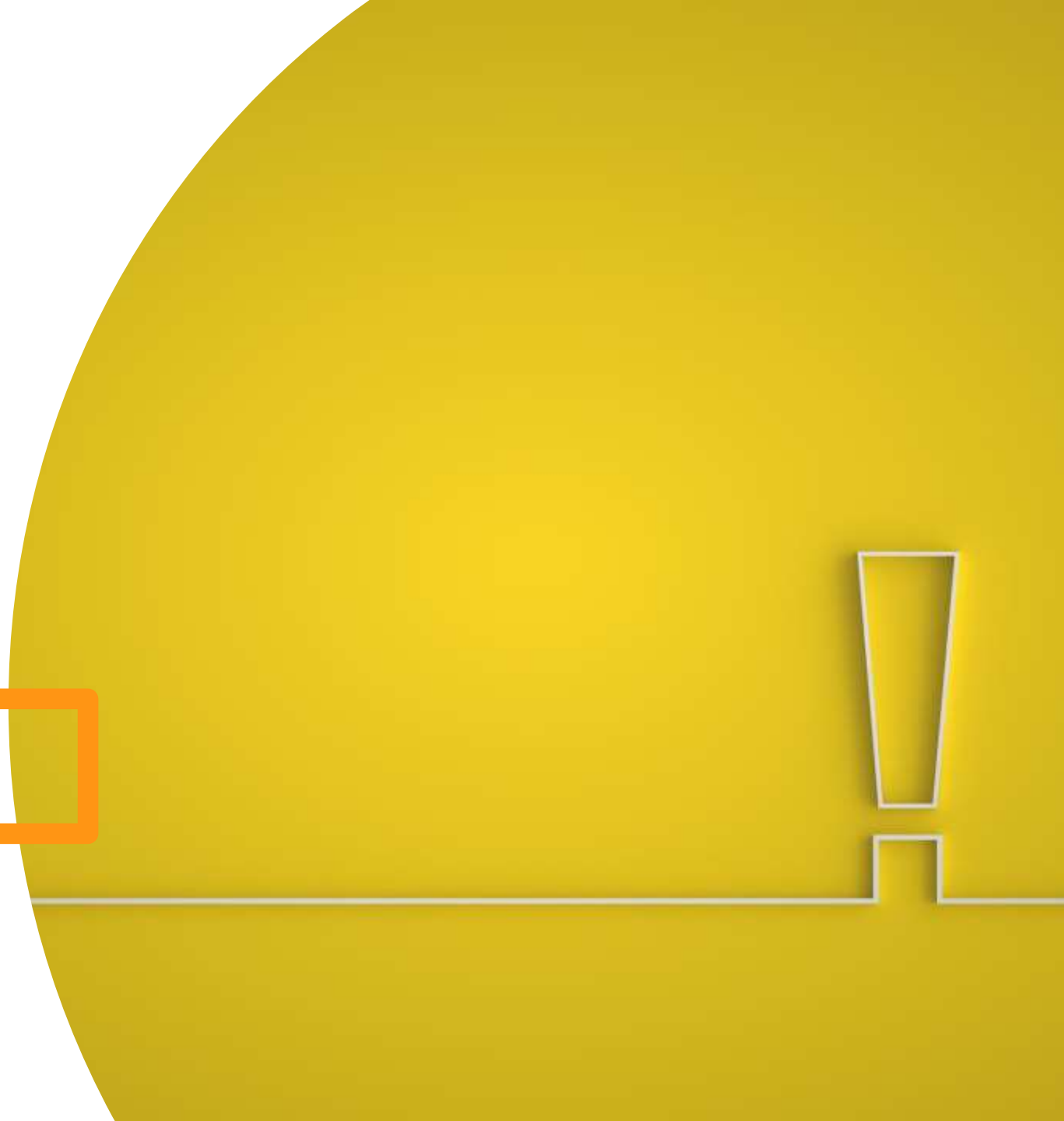
37 | 案例篇：DNS 解析時快時慢，我該怎麼辦？

Hazel Shen



Protocol Stack 關注的網路性能

- 應用層：APP 同時連線數、RPS 、延遲處理、error
  - Wrk, Jmeter: 模擬用戶負載以測試
- 傳輸層：TCP, UDP 工作狀況：connections, reconnection, errors
  - Iperf, netperf
- 網路層: 網路封包的處理能力（Packets Per Second）
  - Pktgen（Linux Kernel 自帶）

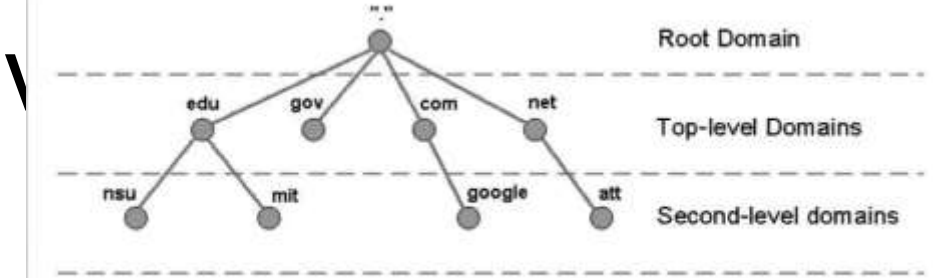
網路最佳化

- 實際上包含整個網路協議的最佳化
- 評估網路性能（e.g. HTTP）：在測試工具中指定 IP 地址

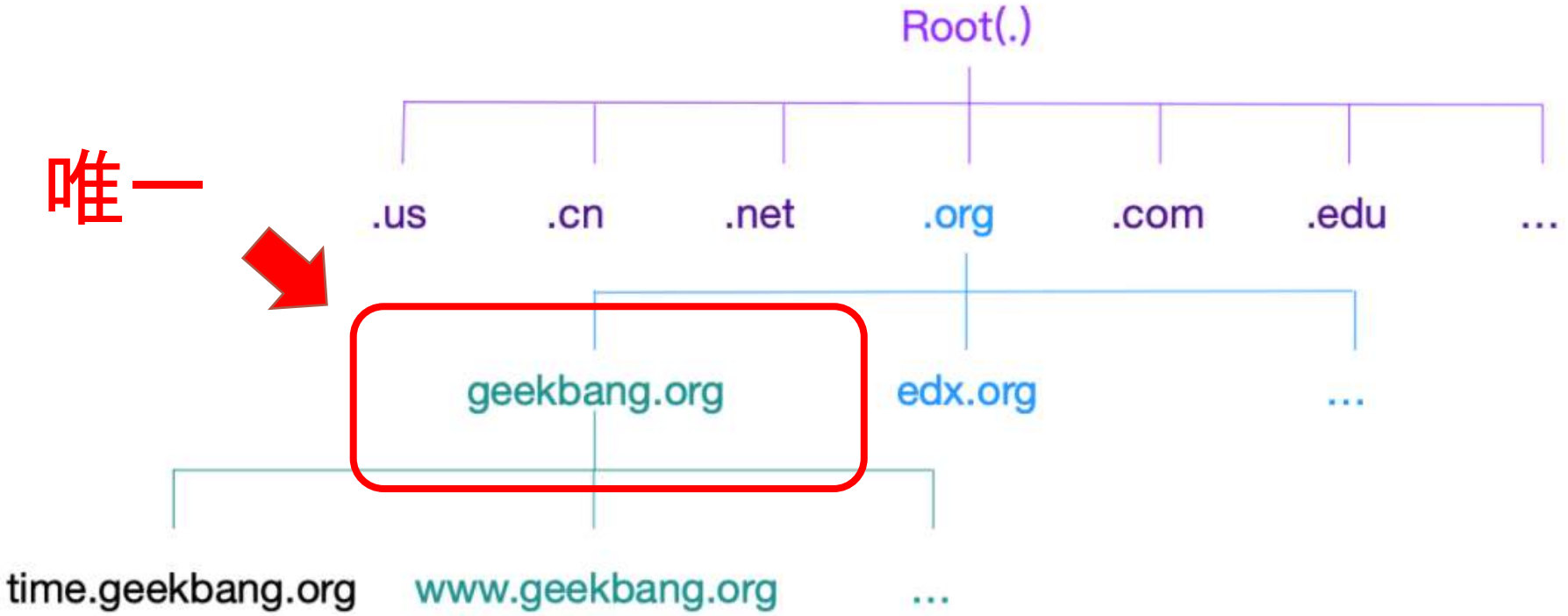
DNS 域名系統

- DNS (Domain Name System)
- Domain Name & IP 映射關係
- 提供應用
  - GSLB: Global Server Load Balance 全域負載均衡
  - 動態服務發現

Domain Name & 解析(Resolv



唯一



DNS 協議

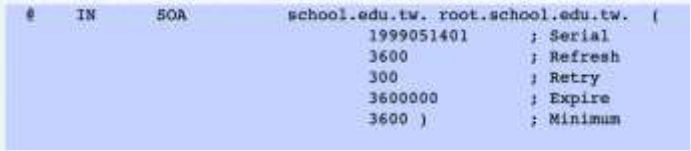
- 在 TCP/IP 中屬於應用層
- 傳輸基於 UDP / TCP
- Server 監聽於 Port 53 之上
- 域名解析以遞迴的方式從頂級域名開始解析
- DNS Server 皆有 Cache，沒有命中才開始查詢

查詢系統配置 – LINUX / Windows

$ cat /etc/resolv.conf

nameserver 114.114.114.114

DNS Resource Record Types

DNS Resource	Description	Examples
A	IPV4	${Server FQDN} IN A 140.123.102.10
AAAA	IPV6	${Server FQDN} 86400 IN AAAA 3ffe: :bbb:93:5
CNAME	alias	www IN CNAME mix
MX	Mail exchanger	${Server FQDN} IN MX 10 mail.twnic.net.tw.
NS	Name Server (不可以 IP 表示)	${Server FQDN} IN NS dns.twnic.net.tw.
SOA	Start of Authority, 每個 Record 只能有一個 SOA, 一定放在第一個	
PTR	定義某個 IP 對應的 Domain Name	${Server FQDN} IN PTR mail.twnic.net.tw.

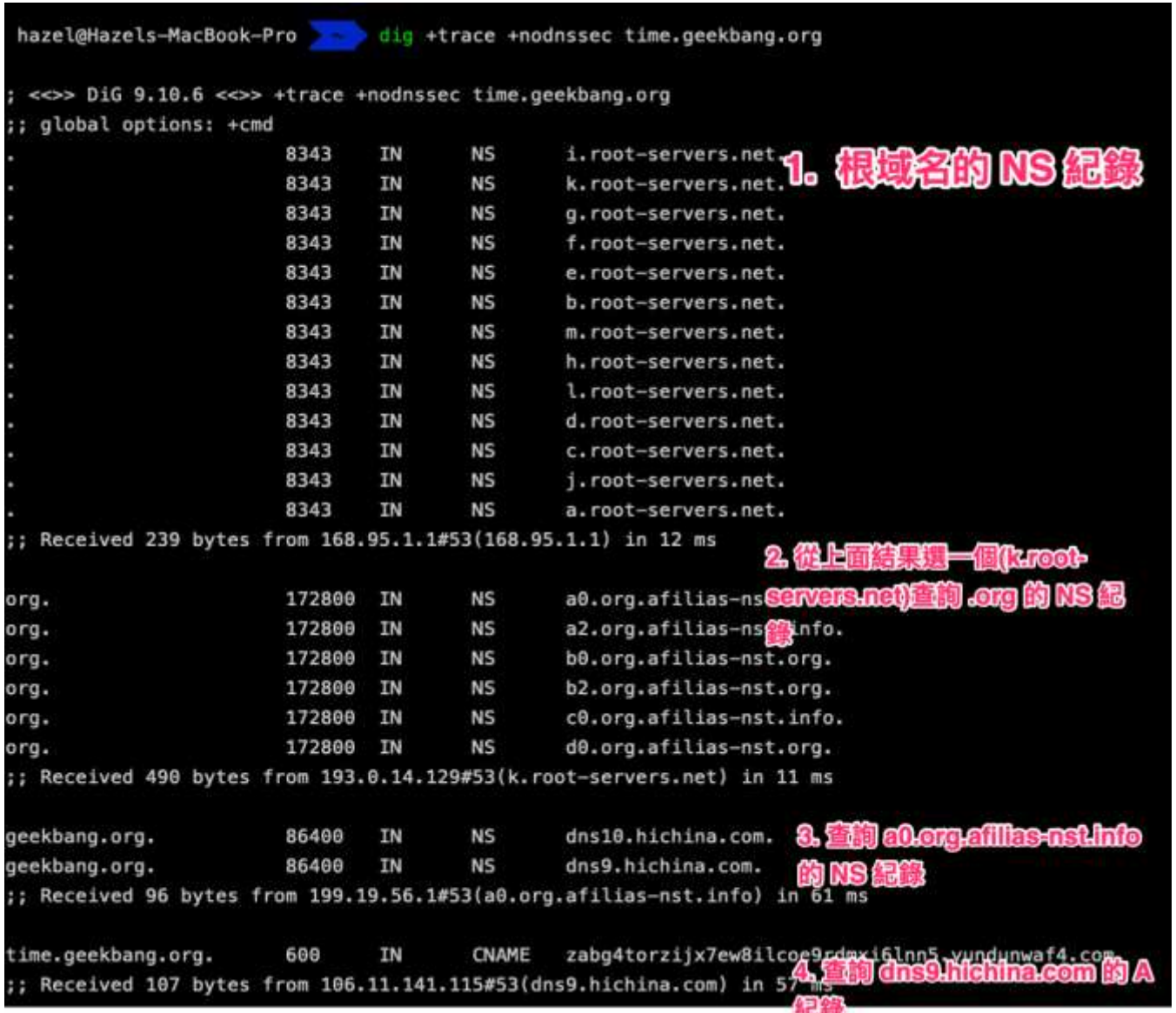
Source: https://zh.wikipedia.org/wiki/DNS%E8%AE%B0%E5%BD%95%E7%B1%BB%E5%9E%8B%E5%88%97%E8%A1%A8

nslookup

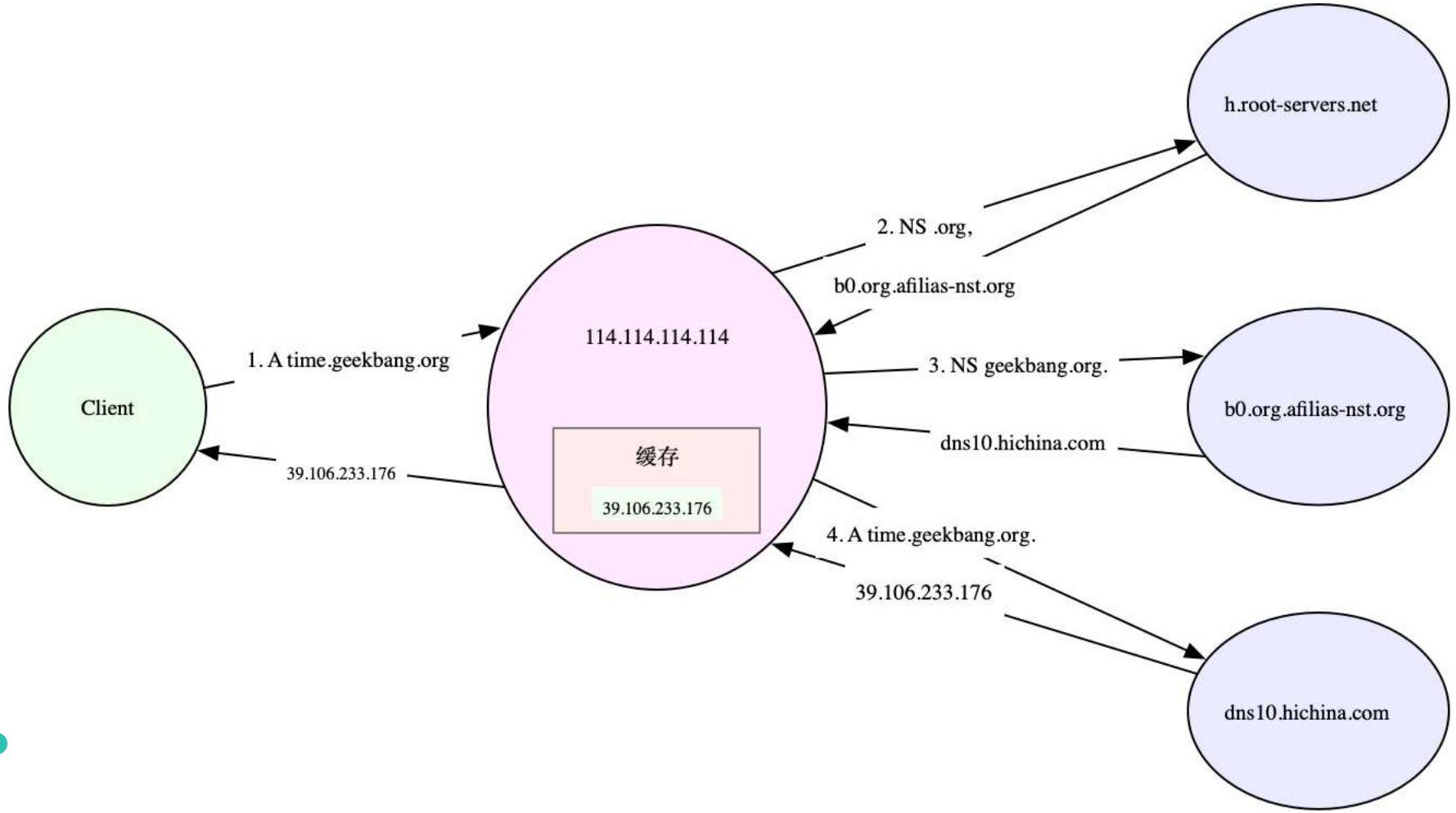
```
✘ hazel@Hazels-MacBook-Pro ~ nslookup time.geekbang.org
Server:         192.168.88.254
Address:        192.168.88.254#53

Non-authoritative answer:
time.geekbang.org       canonical name = zabg4torzijx7ew8ilcoe9rdmxi6lnn5.yundunwaf4.com.
Name:   zabg4torzijx7ew8ilcoe9rdmxi6lnn5.yundunwaf4.com
Address: 47.93.95.233
```

Dig – 可以知道遞迴查詢的結果



遞迴查詢流程圖


h.root-servers.net
2. NS .org,
b0.org.afilias-nst.org
114.114.114.114
Client
1. A time.geekbang.org
3. NS geekbang.org.
b0.org.afilias-nst.org
dns10.hichina.com
缓存
39.106.233.176
39.106.233.176
4. A time.geekbang.org.
39.106.233.176
dns10.hichina.com

區域網路內部的主機名稱 & IP 配對

```
$ cat /etc/hosts
127.0.0.1   localhost localhost.localdomain
::1         localhost6 localhost6.localdomain6
192.168.0.100 domain.com
```

或者可以自行搭建內部的 DNS , 然後指定 DNS Server

```
sudo vim /etc/resolv.conf
```

案例準備I – DNS 解析失敗

- docker pull feisky/dnsutils
- cat /etc/resolv.conf
- $ docker run -it --rm -v $mktemp:/etc/resolv.conf feisky/dnsutils bash

案例準備I – DNS 解析失敗 - 驗證

- /# nslookup time.geekbang.org
- /# ping –c3 ${先前拿到的 name server IP}
- /# cat /etc/resolve.conf //查看 DNS 配置

案例準備II – DNS 解析不穩定

- $ docker run -it --rm --cap-add=NET_ADMIN --dns 8.8.8.8 feisky/dnsutils bash

DNS 解析結果不穩定

- DNS 服務器本身有问题，response time 長 ／ 不穩定
- Client 到 DNS 服務器的 latency 高
- DNS request 或 response packet，在某些情况下被網路設備弄丢

DNS 解析時間太長解法

- DNS cache – dnsmasq, 經常作為 DHCP 服務來使用

- 如何啟動？

  /# /etc/init.d/dnsmasq start

- 如何測試？

/# echo nameserver 127.0.0.1 > /etc/resolv.conf

/# time nslookup time.geekbang.org

小結

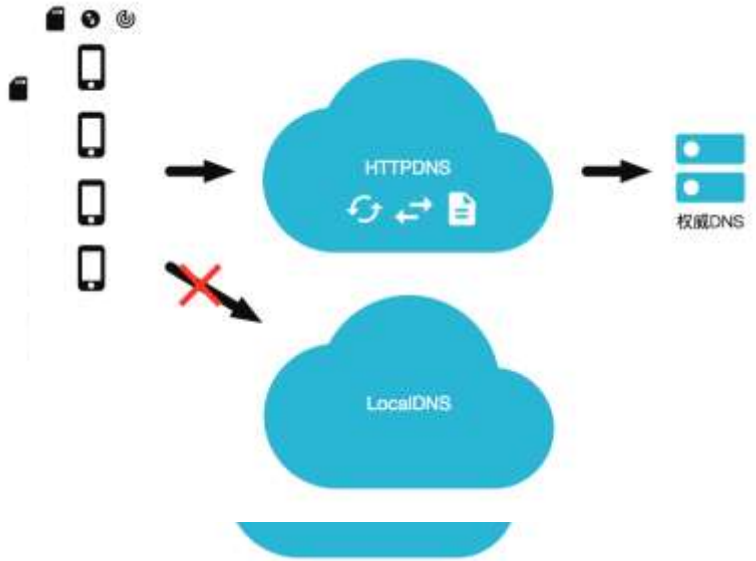
- DNS 作為一個域名和IP配對的查詢服務
- 應用程式沒有考慮 DNS 解析的問題，有時候是 DNS 解析太慢導致的，不一定是應用程式本身的問題
- 常見的 DNS 最佳化方法：
  1. DNS 結果快取
  2. 預先存取 DNS 解析結果
  3. 使用 HTTPDNS 取代常規的 DNS 解析 for 域名劫持問題，使用 HTTP 協議繞過 chain 中的 DNS 服務器
  4. 使用 DNS 的 GSLB，可以提供附載均衡 ／ 高可用，並且可以根據位址給出最近的 IP address

DNS 預存取

- 時機：許多靜態資源但放在各個不同的domain底下
- 作法：在HTML的 <head> 加入 <link rel="dns-prefetch" href="https://my-site.com">
- 限制：DNS Prefetching在https下是無法使用的。若要在https下開啟DNS Prefetching，必須在 <head> 加上 <meta http-equiv="x-dns-prefetch-control" content="on"> 才能啟動DNS Prefetching。但只能啟動連結，而無法啟動手動設定的資源。

HTTPDNS

- 在 DNS 解析前包一層 HTTP 協議
- httpdns的工作原理就是提供給加速客戶一個API接口地址，客戶通過HTTP方式請求此接口地址加上域名參數，回傳客戶端一條 JSON 數組，裡面有該域名所對應的 CDN 邊緣節點的 IP 位址。
- HTTPDNS 調度伺服器接到請求後
- 提供廠商：阿里雲（？



問題思考

你所碰到的 DNS 問題？

碰到過哪些類型的 DNS 問題？

通過哪些方法排查 DNS 問題？
以及如何解決？

Thank You