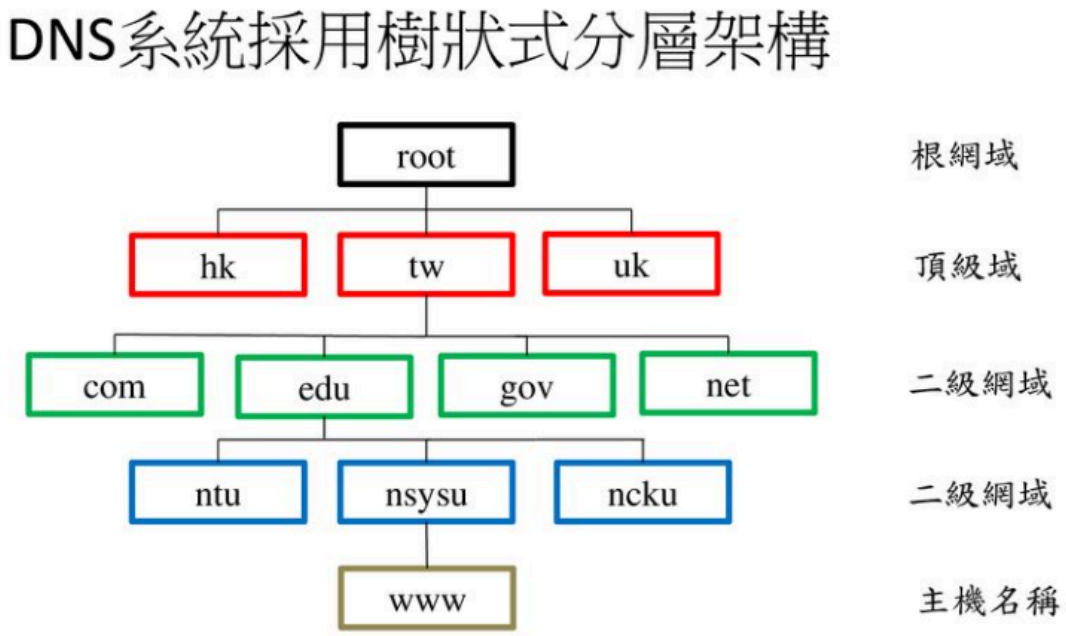
# DNS 是甚麼

- (Domain Name System, 網域名稱系統)
- 我們記名字容易, 但電腦通訊只能靠 **IP** 位址
    - 例子:我們記得 moodle.ncnu.edu.tw, 不太會記 163.22.5.234
- 將 Domain Name 轉換成 IP Address, 讓電腦能找到正確的伺服器
    - 像網際網路的「通訊錄」, 它是把 網域名稱對應到各種「資源紀錄」的系統
        - 像是把好記的名字轉換成數字 IP

## 樹狀階層式架構




ref
咪聽小紀錄

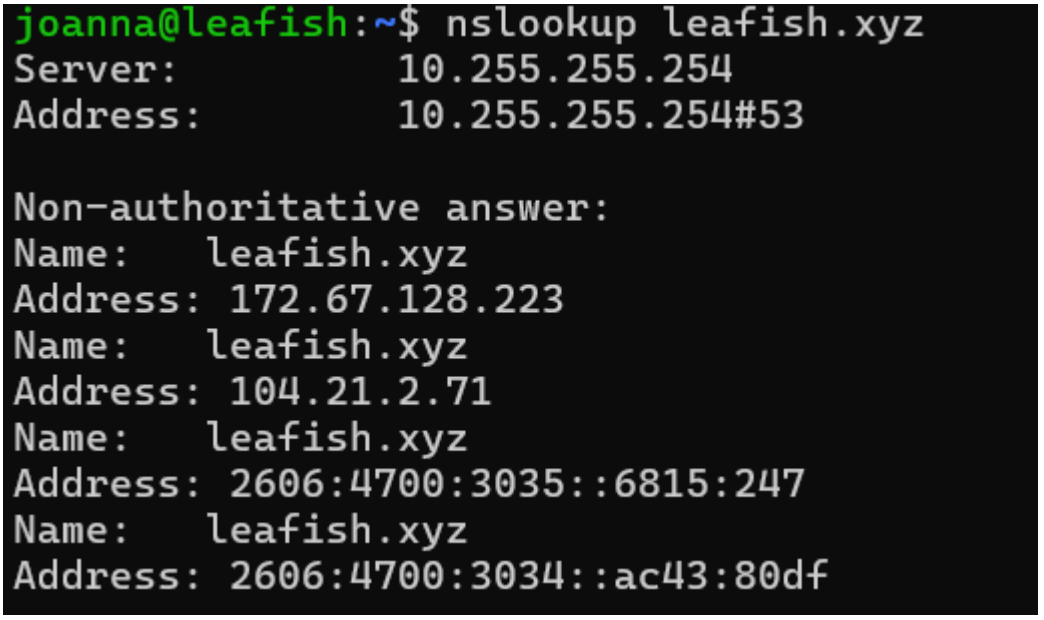
FIXME: 界定什麼 Domain 被誰管
原本要從 root 找 -> 一層一層往下
-> 這樣查詢流量報掉
先設定 DNS Server -> 會先找自己, 找不到去外面找
! 他是樹狀, 但現在會有前輩幫你查回來 (單純 DNS Server 只管自己的紀錄, 不會幫忙問)
現在有支援幫查功能才會幫你查
DNS Server:1. 紀錄 DNS 的 2. 幫我找 IP 到底是什麼的 resolver(?) -> 能力可並存, 也可單獨

DNS Server 有沒有開啟 forwarding 的功能 ( 基本只管好自己 )

- 域名從「右到左」一層一層往下, ex. moodle.ncnu.edu.tw.
    - . → 世界的 13 台 root DNS (最右邊的 . 通常被省略)

    - `.tw` → 頂級域名 (TLD)
    - `.edu.tw` → 二級域名（教育單位）
    - `ncnu.edu.tw` → 校園網域
    - `moodle.ncnu.edu.tw` → 完整主機（Moodle 系統）
- FQDN (完整網域名稱，Fully Qualified Domain Name)
    - FQDN = Host name + Domain name
        - Host name = `moodle`
        - Domain name = `ncnu.edu.tw`
- FQDN 就是樹狀結構中「從根到某一節點的完整路徑」

### nslookup 指令

- nslookup 查詢特定網域的 DNS 紀錄
    - `nslookup <Domain Name>`
        - 


# DNS 查詢步驟

一、先看本機紀錄

1. 應用程式層的快取
    - 例如 Chrome/Firefox 都有「Host resolver cache」
        - 把最近查過的 網域→**IP** 結果暫存起來，依照 TTL 保留一段時間，以便下次更快找到 IP、減少對外 DNS 查詢
        - 如果有命中，就不會再往下查
2. Stub resolver (作業系統的 resolver（解析器))
    - 依 `/etc/nsswitch.conf` 來看
        - 定義了解析的依序優先順序，決定先要使用 /etc/hosts 還是 /etc/resolv.conf 的設定

```
joanna@joanna-VirtualBox: ~
joanna@joanna-VirtualBox:~$ cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd
group:          files systemd
shadow:         files
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

- files 指本機檔案：ex. /etc/hosts、/etc/passwd

○ 查 files → /etc/hosts

```
joanna@joanna-VirtualBox:~$ cat /etc/hosts
127.0.0.1       nginx1.load.com
127.0.0.1       proxynginx
127.0.0.1       localhost
127.0.1.1       joanna-VirtualBox
# The following lines are desirable for IPv6 capable hos
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

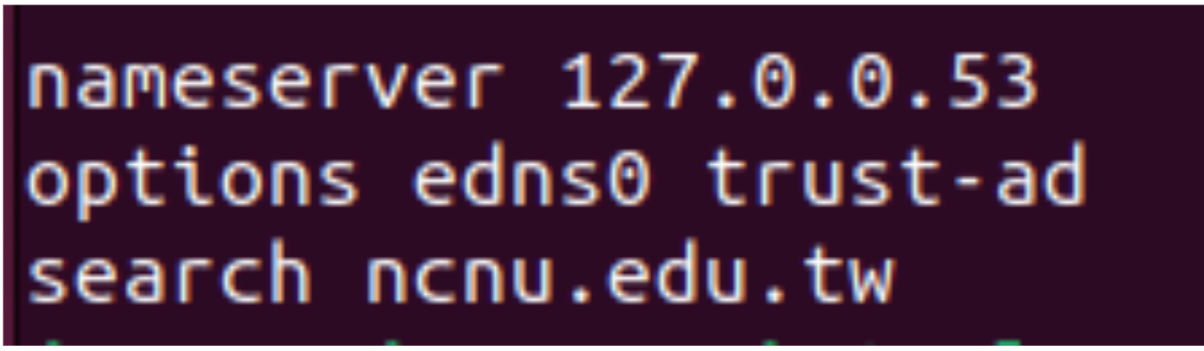
○ 查 mdns4_minimal → .local 等 mDNS 名稱

- 解析以 .local 結尾的主機名時，不會去 DNS，而是透過區域網路的 multicast DNS 來找到對應的設備
- ex. ping raspberrypi.local → 呼叫 mdns4_minimal → 用 multicast DNS 在區網廣播問「誰是 pi.local？」→ 樹莓派回覆 → 解析成功

○ 查 dns → 需要時才交給 DNS 伺服器

**二、查 DNS Server**

- 查詢 Linux 設定的 DNS，如：/etc/resolv.conf 檔案
  - 決定要問哪台 DNS

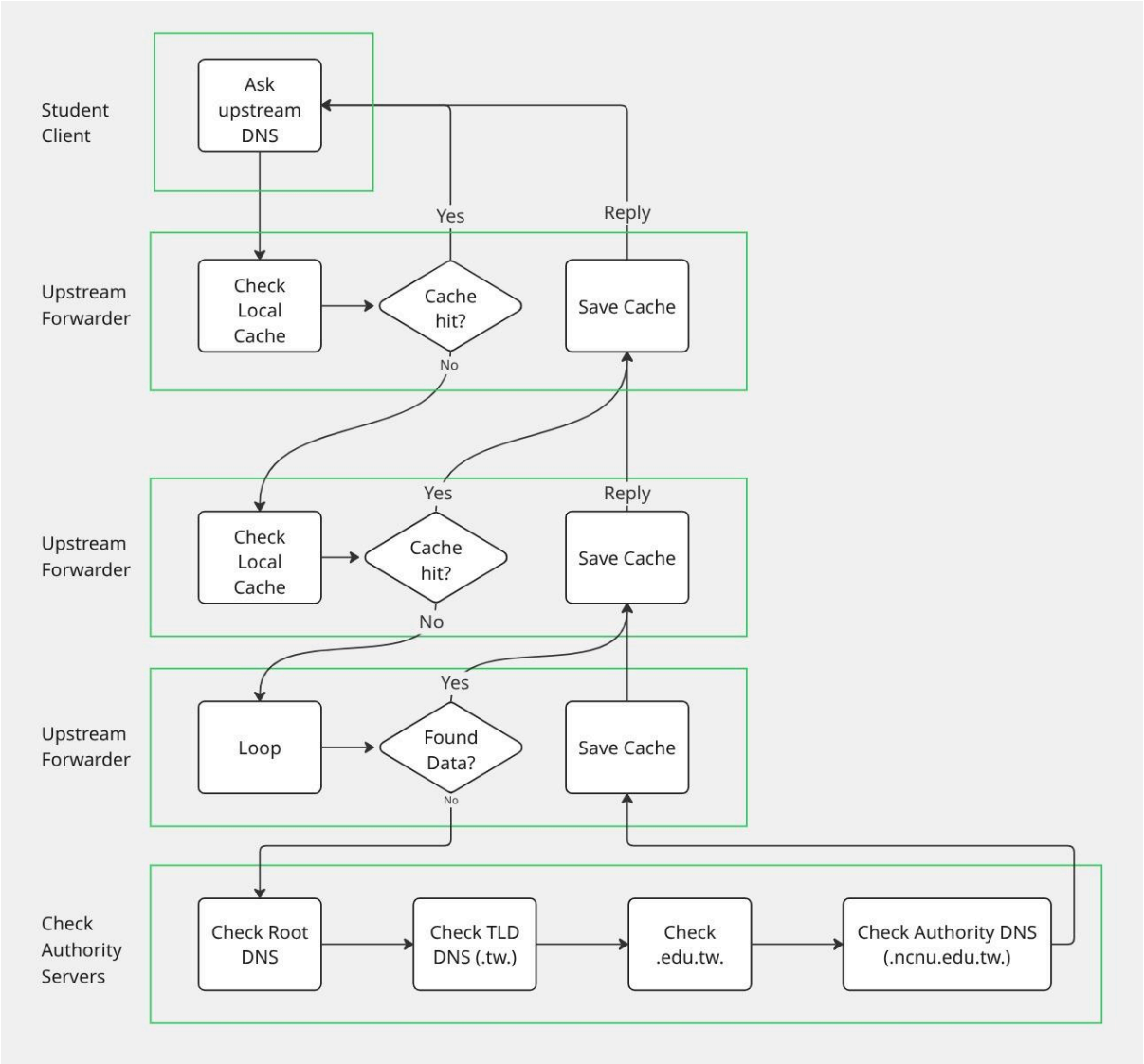
    - 

        - nameserver 127.0.0.53：系統把 DNS 查詢先送到本機的 127.0.0.53 (統一入口)，然後再轉送到真正的上游 DNS
        - search ncnu.edu.tw：定「搜尋網域」。當你查一個不含點的短名稱（例如 host1）時，解析器會先嘗試 host1.ncnu.edu.tw
- Forwarder（DNS 轉送器）
    - 收到 DNS 查詢後再幫忙轉送到「上游遞迴解析器」，並把結果回給下游
    - 好處：
        - 集中管理：黑白名單、DNSSEC 驗證等
        - 速度快：上游遞迴器通常硬體更好、快取記憶體更大，有結果直接回傳，不用遞迴解析
        - 條件式轉送：內外網域分流。如`*.school.edu`找 10.0.0.53，其餘外部網域找公共遞迴器
- **DNSSEC**

網域名稱系統 (DNS) 像網際網路的電話簿，他會告訴電腦向哪裡傳送資訊，以及從哪裡拿資訊。不過，DNS 也接受網際網路提供的任何位址，而不會進行任何詢問。

DNSSEC 為一個通訊協定，透過提供驗證，在 DNS 之上又增加了一層信任。

    - DNSSEC 對現有 DNS 記錄新增加密簽章，藉此保護網域名稱系統的安全
    - 新增了一些新的 **DNS** 記錄類型，之後會提到
- 遞迴解析 (Recursive resolver)
    - 沒有使用 forwarder（或 forwarder 也沒快取，需要遞迴）
    - 往 root 查 → 往 .tw 查 → 往 edu.tw 查 → 往 ncnu.edu.tw 查 → 查到 moodle.ncnu.edu.tw
    - 就會得到 IP 💯




**Resolver**（解析器）**& Forwarder**（轉送/代理）

**Resolver**（解析器）：負責替用戶端把名稱解析成 DNS 記錄的東西

- Stub resolver：在作業系統或應用程式中。只將查詢轉發到預先配置的 DNS 伺服器。
- Recursive resolver：全功能遞迴解析器（如 8.8.8.8）。會自己去 Root → TLD → 權威查到底，並快取結果。
- Root and TLD Servers：全世界已知（13 個根伺服器），並將遞迴解析器導向到正確的 DNS 區域。

**Forwarder**（轉送/代理）：網路中的 DNS 伺服器，不自行遞迴，而是把收到的查詢轉送給上游遞迴解析器處理；本身通常也會快取。

# DNS 記錄類型

較常見的 **DNS** 記錄類型

| 紀錄名稱 | 用途 |
| --- | --- |
| A | 儲存網域 IP 位址的記錄 |
| AAAA | 網域的 IPv6 位址的記錄 |
| CNAME | 將一個網域或子網域轉寄到另一個網域，不提供 IP 位址 |
| MX | 將郵件導向到電子郵件伺服器 |
| TXT | 可讓管理員在該記錄中儲存文字註解。通常用於電子郵件安全 |
| NS | 儲存用於 DNS 項目的名稱伺服器 |
| SOA | 儲存有關網域的管理資訊 |
| SRV | 指定用於特定服務的 port |
| PTR | 在反向查詢中提供網域名稱 |

- A 紀錄：網域的 **IPv4** 位址
  - | example.com | 記錄類型： | 值： | TTL |
    | --- | --- | --- | --- |
    | @ | A | 192.0.2.1 | 14400 |
  - 「@」符號表示這是根網域的記錄
  - 「192.0.2.1」為 example.com 的 IPv4 位址
  - 「14400」值是 TTL（存留時間），以秒為單位
- AAAA 紀錄：網域的 **IPv6** 位址
  - | example.com | 記錄類型： | 值： | TTL |
    | --- | --- | --- | --- |
    | @ | AAAA | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 14400 |
  - 與 A 記錄一樣，AAAA 記錄讓用戶端裝置能夠瞭解網域名稱的 IP 位址，紀錄的是 IPv6 位址
  - 由於 IPv4 位址僅有 2^32 個，且其中有一些是保留或無法用來分配的（例如網段的網路位址、廣播位址、私有位址範圍等），所以快被用完了，才有 IPv6 (2^128 個)
- CNAME 紀錄：網域別稱的感覺
  - 所有 CNAME 記錄都必須指向一個域，絕不能指向 IP 地址
  - 像一個尋寶遊戲，每個線索都指向另一個線索，最後的線索指向寶藏。
    - 帶有 CNAME 記錄的域名就像一條線索，可以指向另一個線索（另一個具有 CNAME 記錄的域名）或寶藏（具有 A 記錄的域名）
  - 讓一個網站可能有很多入口！

| 類型 ⓘ | 名稱 ⓘ | 內容 ⓘ |
|---|---|---|
| CNAME | leafish.xyz | leafishweb.pages.dev |

- MX 紀錄：將電子郵件導向至郵件伺服器

| example.com | 記錄類型： | 優先順序： | 值： | TTL |
|---|---|---|---|---|
| @ | MX | 10 | mailhost1.example.com | 45000 |
| @ | MX | 20 | mailhost2.example.com | 45000 |

  - 網域前面的「優先順序」數字表示偏好，越小代表越優先
    - 伺服器將始終先嘗試 mailhost1，因為 10 小於 20。當循序傳送失敗時，伺服器將預設使用 mailhost2。
    - 幫助兩個郵件伺服器之間做負載平衡
- TXT 記錄：讓網域管理員在 DNS 伺服器上留下註解
  - TXT 記錄最初的目的是用作存放人類可讀筆記的地方。但現在也可以將一些機器可讀的資料放入 TXT 記錄中。

| 類型 ⓘ | 名稱 ⓘ | 內容 ⓘ |
|---|---|---|
| TXT | leafish.xyz | "v=spf1 include:icloud.... |
| TXT | leafish.xyz | apple-domain=DAT2H... |

  - 給機器讀（主要用途）：
    - SPF（郵件驗證機制）→ 規定哪些伺服器可以替這個網域寄信
      - ex：`v=spf1 include:icloud.com ~all`
        - 代表這個網域的郵件信任 iCloud 的伺服器寄出 → 只有 iCloud 的郵件伺服器有權利替 leafish.xyz 寄信
        - ⚠ 只驗證「寄信的伺服器」，不能保證信件內容沒被改
    - DKIM（郵件簽章驗證）→ 用公鑰簽名驗證郵件來源
      - 驗證「信件內容有沒有在傳送過程中被竄改」
      - 寄信伺服器在郵件標頭加上 數位簽章。
      - 收件伺服器去查寄件網域 DNS 的 TXT 記錄（裡面有公鑰）。
      - 用公鑰驗證簽章 → 確認信件確實是這個網域寄出，且內容完整。
      - ⚠ 只驗證「寄件者真的控制這個網域」+「內容沒改」，但沒規定收件方怎麼處理驗證失敗
    - DMARC（郵件策略）→ 指示郵件伺服器如何處理 SPF/DKIM 驗證失敗的信件
      - ex：`v=DMARC1; p=reject; rua=mailto:report@leafish.xyz`
        - p=reject → 驗證失敗就拒收
          - none → 只是收集報告，不做動
          - quarantine → 視為垃圾郵件
          - reject → 直接拒收
        - rua=... → 要把驗證失敗的報告寄到哪裡

        - Domain Ownership Verification（網域所有權驗證）
            - 確保「你真的擁有這個網域的管理權」
            - 在 DNS 裡新增一條 TXT 記錄，內容是一串 token，代表你是網域的管理員，才允許你用它來做 iCloud 郵件服務
- NS 紀錄：用來指定「這個網域/子網域的權威 DNS 伺服器是哪些」
    - | example.com | 記錄類型： | 值： | TTL |
      |---|---|---|---|
      | @ | NS | ns1.exampleserver.com | 21600 |
    - 代表 ns1 是 example.com 的權威 DNS，想查這個網域的 A/AAAA/MX…等紀錄，請去問 ns1 伺服器
- SOA 記錄：儲存有關網域或區域的重要資訊
    - 例如系統管理員的電子郵件地址、上次更新網域的時間
    - | 姓名 | example.com |
      |---|---|
      | 記錄類型 | SOA |
      | MNAME | ns.primaryserver.com |
      | RNAME | admin.example.com |
      | SERIAL | 1111111111 |
      | 重新整理 | 86400 |
      | RETRY | 7200 |
      | EXPIRE | 4000000 |
      | TTL | 11200 |
- SRV 記錄：紀錄給特定的服務指定主機和 port

  DNS 記錄只指定一個伺服器或一個 IP 位址，但 SRV 記錄還包括該 IP 位址的一個 port

    - 非必要紀錄 哈哈
    - | 服務 | XMPP |
      |---|---|
      | 通訊協定* | TCP |
      | 名稱** | example.com |
      | TTL | 86400 |
      | class | IN |
      | 類型 | SRV |
      | 優先順序 | 10 |
      | 權數 | 5 |
      | 連接埠 | 5223 |
      | 目標 | server.example.com |
- PTR 紀錄：用於反向解析（reverse DNS）
    - 提供與 IP 位址相關聯的網域名稱 (IP → 主機名)，常見用途：

    - 反垃圾郵件：許多收件郵件伺服器會檢查寄信來源 IP 是否有合理的 PTR，沒有或不合理的 PTR，常被視為垃圾郵件來源。
    - 日誌記錄：系統記錄檔通常只會記錄 IP 位址；反向 DNS 查閱可以將這些位址轉換為網域名稱，來更易於閱讀記錄檔。

# DNSSEC

- DNSSEC 為一個通訊協定，對現有 DNS 記錄新增加密簽章，在 DNS 之上又增加了一層信任。
- 傳統 DNS 多用 UDP/53 port、資料不加密也無簽章 → 容易被偽造回應/快取汙染（攻擊者可以搶先丟假的答案給你的 DNS）。
- 為了防止 DNS 回覆被竄改（提供資料完整性與來源認證，非加密傳輸內容）

**DNSSEC** 常見的 **DNS** 記錄類型

| 紀錄名稱 | 用途 |
| --- | --- |
| RRSIG | 包含加密簽章 |
| DNSKEY | 包含公共簽名金鑰 |
| DS | 包含 DNSKEY 記錄的雜湊 |
| NSEC 和 NSEC3 | 用於明確否認 DNS 記錄的存在 |
| CDNSKEY 和 CDS | 用於請求對父區域中的 DS 記錄進行更新的子區域 |

**DNSSEC** 機制 **=**「簽章 **+** 信任鏈」

- 就像是公機關（example.com）準備兩種章：
    - 業務章（ZSK）：簽每份公文內容（RRset）→ 產生對應簽章紀錄（RRSIG）
    - 大章（KSK）：蓋在「印鑑卡」（DNSKEY）上 → 產生對應簽章紀錄（RRSIG）
        - 「印鑑卡」：指印鑑證明，像這顆印章的「身分證」


- 上級機關(.com)留存這枚大章(KSK)的印鑑存根(DS) → 留紀錄(內含 DNSKEY 的雜湊)

1. 用戶端發問(帶要驗證的請求)
    - 你向「公文服務窗口」(遞迴解析器)說:我要文件,且要看章(請附簽章與憑證)。
2. 權威回覆「資料 + 簽章」
    - 承辦單位把公文內容(RRset)連同承辦章(RRSIG) (RRset 跟 RRSIG 用的業務章互相對應),一起給你;還附上印鑑卡(DNSKEY)。
3. 驗證信任鏈

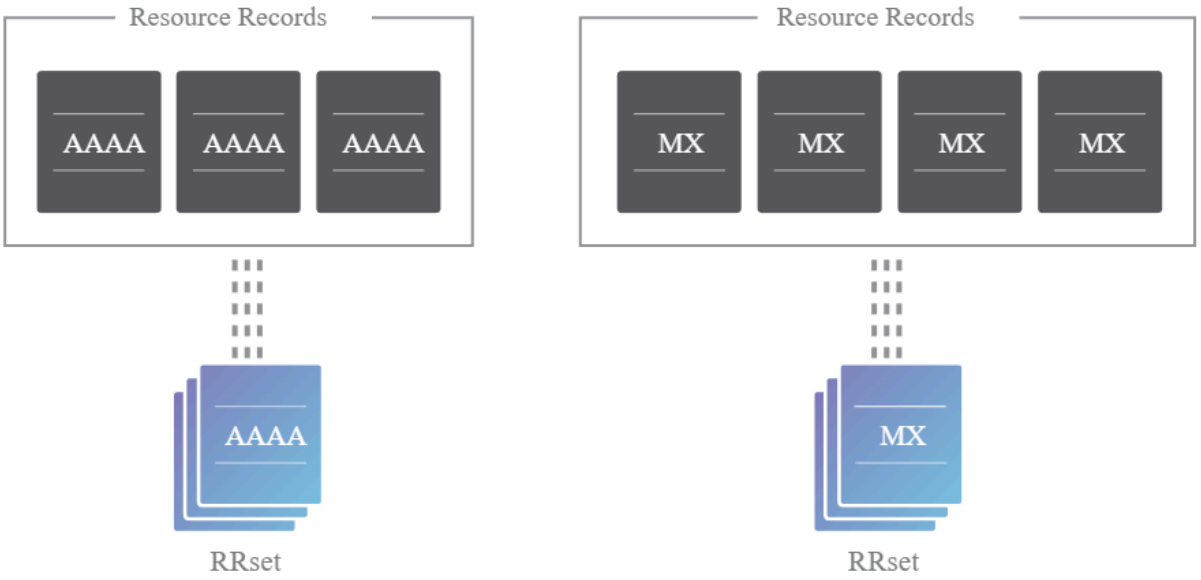
- 先比對:公文章(RRSIG)是否吻合承辦單位的印鑑卡(DNSKEY)。
- 再比對:印鑑卡是否與上級機關存根(DS)一致;一路比到最高機關的名冊(Root)。
- 任何一關對不起來:退件(SERVFAIL)。

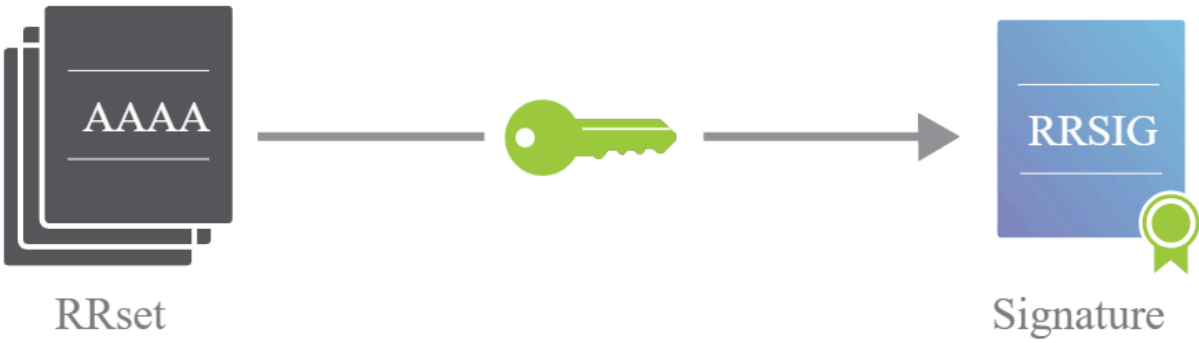
[How DNSSEC Works]

使用機制

使用機制

1. 將所有相同類型的記錄分組到一個資源記錄集(RRset)中
    - ex. 有三個具有相同名稱與類型,的 MX 記錄,它們將全部綁到一個 MX RRset

    - 會是整個 RRset 獲得數位簽章，而不是單獨的 DNS 記錄獲得
    - 

2. DNSSEC 中的每個區域都有一個區域簽名金鑰配對 (ZSK)＝私鑰＋公鑰（公鑰會出現在該區域的 DNSKEY 記錄中）
    - 使用專用 ZSK 為每個 RRset 建立數位簽章，簽完後稱為 RRSIG，記錄儲存在名稱伺服器中
3. 代表這些是我的 DNS 記錄，它們來自我的伺服器，他們應該長這樣
    - 


# DNS 相關角色

## Registrar（註冊商）

- 可以買網域的店家
    - 例如：Cloudflare、GoDaddy、Google Domains
- `whois <Domain Name>`
    - 用來查詢網域名稱和 IP 的服務
    - 查網域的註冊資料

```
joanna@joanna-VirtualBox:~$ whois leafish.xyz
Domain Name: LEAFISH.XYZ
Registry Domain ID: D439480986-CNIC
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: http://cloudflare.com
Updated Date: 2025-03-06T04:26:27.0Z
Creation Date: 2024-03-11T09:36:30.0Z
Registry Expiry Date: 2026-03-11T23:59:59.0Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: TROY.NS.CLOUDFLARE.COM
Name Server: MELINDA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: registrar-abuse@cloudflare.com
Registrar Abuse Contact Phone: +1.4153197517
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-10-01T18:19:48.0Z <<<
```

  - 網域：leafish.xyz
  - 註冊商：Cloudflare, Inc.
  - 註冊日：2024-03-11
  - 最近更新：2025-03-06
  - 到期日：2026-03-11
  - DNS 伺服器：TROY.NS.CLOUDFLARE.COM、MELINDA.NS.CLOUDFLARE.COM
    → 使用 Cloudflare 的權威 DNS
  - DNSSEC：`unsigned` → 目前未啟用 DNSSEC

- `dig <Domain Name>`
  - 從 DNS 伺服器查詢 DNS 記錄資訊
    - ex. A 記錄、MX 記錄等

```
joanna@joanna-VirtualBox:~$ dig leafish.xyz

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> leafish.xyz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43707
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:  提出的問題
;leafish.xyz.                   IN      A

;; ANSWER SECTION:  回答問題
leafish.xyz.            300     IN      A       104.21.2.71
leafish.xyz.            300     IN      A       172.67.128.223

;; Query time: 44 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Oct 02 02:23:44 CST 2025
;; MSG SIZE  rcvd: 72
```

- `host <Domain Name>`
  - 也查 DNS 記錄，但輸出簡潔

- 
```
joanna@leafish:~$ host www.ncnu.edu.tw
www.ncnu.edu.tw has address 163.22.12.5
www.ncnu.edu.tw has IPv6 address 2001:e10:6840:12:163:22:12:20
```
- `host <ip>`
  - 做反向 DNS（IP → 名稱，查 PTR 記錄）
  - 
```
joanna@leafish:~$ host 8.8.8.8
8.8.8.8.in-addr.arpa domain name pointer dns.google.
```

**NS（Authoritative Name Server，權威名稱伺服器）**

- 

### Cloudflare 名稱伺服器

Cloudflare 上的每個 DNS 區域都指派了一組 Cloudflare 品牌標誌的名稱伺服器。

| 類型 | 值 |
| --- | --- |
| NS | melinda.ns.cloudflare.com |
| NS | troy.ns.cloudflare.com |

  - Cloudflare 畫面

- 
```
joanna@leafish:~$ dig leafish.xyz NS

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> leafish.xyz NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44004
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;leafish.xyz.                   IN      NS

;; ANSWER SECTION:
leafish.xyz.            2820    IN      NS      melinda.ns.cloudflare.com.
leafish.xyz.            2820    IN      NS      troy.ns.cloudflare.com.
```
  - 也可用 dig 來查詢

  - 圖中兩個權威名稱伺服器都會回覆 DNS 查詢