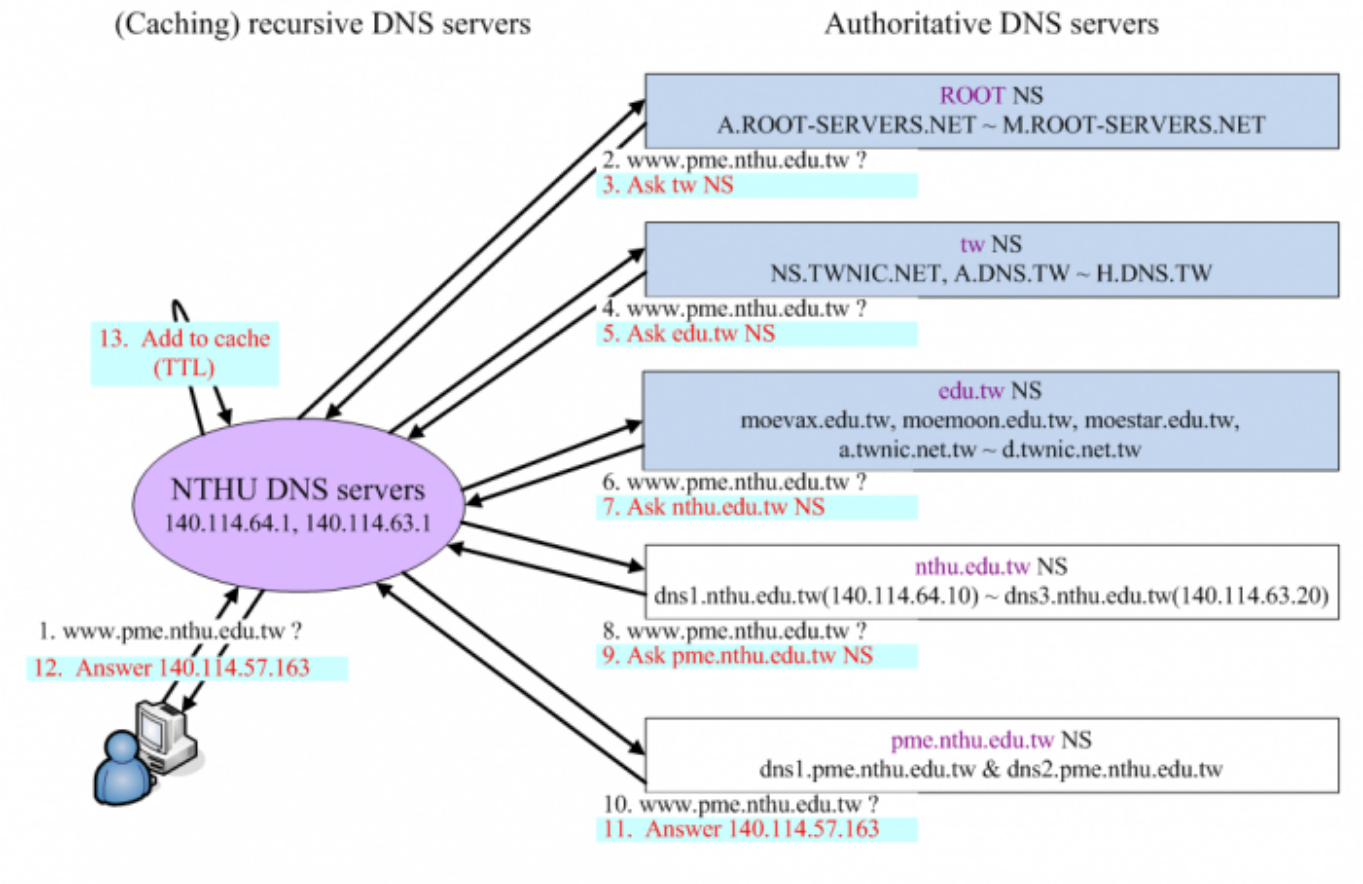
DNS 記錄之解答過程

- 網際網路上資料封包的傳送要有目的端的 IP 位址才能送達，但 IP 位址對人們而言並不好用，例如：我們通常不會去記清華大學首頁的 IP 位址，但記網域名稱(domain name) www.nthu.edu.tw顯然容易多了（即使用搜尋引擎，大概也不會去記搜尋引擎的 IP 位址）。那電腦如何找到目的端的 IP 位址，這就得仰賴 DNS 服務所提供的查詢服務，因此，若電腦上未能正確設定 DNS 伺服器，該部電腦就無法建立任何用網域名稱的連線。
- DNS 為網際網路服務 (Internet service) 重要的基礎之一，當 DNS 記錄無法順利查詢時，多數使用者會認為網路出狀況，但要釐清問題的原因並不容易，因為整個 DNS 運作架構是一個龐大、複雜的分散式系統，由全世界各地的網管人員分工合作來管理維護。
- 下圖**僅以查詢 www.pme.nthu.edu.tw 的 IPv4 位址 (A record) 為例**DNS 尚有其他多種記錄，如MXCNAMEPTR等，雖不在本文所舉的例子範圍內，但其查詢過程亦同。），來介紹 DNS 記錄之解答過程(resolving process)說明電腦與 DNS 伺服器如何運作。



各步驟說明

1. 電腦對 Recursive DNS 伺服器 140.114.64.1 （此由該台電腦的設定所決定）送出查詢 www.pme.nthu.edu.tw 的 IPv4 位址的請求（以下簡稱此查詢）。
2. Recursive DNS 伺服器 140.114.64.1 對 ROOT NS (name server因 140.114.64.1 伺服器本身有 ROOT NS 的 IP 位址設定資料）送出此查詢。
3. ROOT NS 無此查詢答案，回覆告知授權區域(authoritative zone) tw 的 NS 資料。

模擬第2、3步過程之操作指令如下：

```
# dig @a.root-servers.net www.pme.nthu.edu.tw
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 12
```

```
;; QUESTION SECTION:
;www.pme.nthu.edu.tw.           IN      A
;; AUTHORITY SECTION:
tw.                    172800  IN      NS      A.DNS.tw.
...
;; ADDITIONAL SECTION:
A.DNS.tw.              172800  IN      A       203.73.24.8
...
;; Query time: 143 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
```

4. 140.114.64.1 轉向 tw NS 送出此查詢。
5. tw NS 無此查詢答案，回覆告知授權區域 edu.tw 的 NS 資料。
6. 140.114.64.1 轉向 edu.tw NS 送出此查詢。
7. edu.tw NS 無此查詢答案，回覆告知授權區域 nthu.edu.tw 的 NS 資料。
8. 140.114.64.1 轉向 nthu.edu.tw NS 送出此查詢。
9. nthu.edu.tw NS 無此查詢答案，回覆告知授權區域 pme.nthu.edu.tw 的 NS 資料。
10. 140.114.64.1 轉向 pme.nthu.edu.tw NS 送出此查詢。
11. pme.nthu.edu.tw NS 有此查詢答案，回覆告知www.pme.nthu.edu.tw 的 IPv4 位址為 140.114.57.163

模擬第10、11步過程之操作指令如下：

```
# dig @dns1.pme.nthu.edu.tw. www.pme.nthu.edu.tw
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;www.pme.nthu.edu.tw.           IN      A
;; ANSWER SECTION:
www.pme.nthu.edu.tw.    86400   IN      A       140.114.57.163
```

12. 140.114.64.1 將此查詢答案回覆該台電腦。
13. 140.114.64.1 將此查詢結果放入暫存空間 (cache)，下次相同的查詢則可以直接回答，不用去外界查，而資料暫存的時間不會超過該筆資料的 TTL (Time-to-live) 設定值。

補充說明

(Caching) recursive DNS server

1. 提供 DNS 查詢服務，負責將客戶的查詢，從根找到正確的授權答案給客戶。
2. **最好限定客戶 IP 來源，不要對整個 Internet 開放**，以避免成為 DNS DDoS Attack 的打手；同時減少 DNS cache poisoning 的機會。因此，**本中心之 recursive DNS 伺服器 140.114.63.1 與 140.114.64.1 僅限提供本校 IP 使用**。

Authoritative DNS server

1. 負責登記授權區域(zone) 的最新、最正確 DNS 記錄(record)資料；同時回答來自 Ineternet 各方詢問該授權範圍的 DNS 查詢 (query)，最好不要回答非授權範圍內的查詢，**建議與(Caching) recursive DNS server 分開建置，以提高安全性**。因此，本中心之 authoritative DNS 伺服器 140.114.63.10, 140.114.63.20 與 140.114.64.10 僅回答本中心授權範圍的 DNS 查詢，若使用者錯誤將之設定為個人電腦用的 DNS 伺服器，將無法正常進行 DNS 查詢工作。

- 不回答非授權範圍內的查詢。

```
# dig @dns1.nthu.edu.tw www.mit.edu

; <<>> DiG 8.3 <<>> @dns1.nthu.edu.tw www.mit.edu
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 4
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      www.mit.edu, type = A, class = IN

;; Total query time: 0 msec
;; FROM: mx to SERVER: dns1.nthu.edu.tw  140.114.64.10
;; WHEN: Tue May 19 16:03:27 2009
;; MSG SIZE  sent: 29  rcvd: 29
```

2. 為提高服務可用性，**最好有兩台(含)以上同時提供服務，採 Master/Slave 架構**，由 master 保有原始的 DNS 記錄(record)資料，slave 透過 zone transfer 由 master 獲得備份的資料。
3. **上下層授權的 NS 資料最好一致**，以減少發生問題的機會。
   - nthu.edu.tw NS 授權 pme.nthu.edu.tw NS 為 dns1.pme.nthu.edu.tw. 與 dns2.pme.nthu.edu.tw. 兩筆。

```
# dig @dns1.nthu.edu.tw pme.nthu.edu.tw ns

; <<>> DiG 8.3 <<>> @dns1.nthu.edu.tw pme.nthu.edu.tw ns
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      pme.nthu.edu.tw, type = NS, class = IN

;; AUTHORITY SECTION:
pme.nthu.edu.tw.        1D IN NS        dns1.pme.nthu.edu.tw.
pme.nthu.edu.tw.        1D IN NS        dns2.pme.nthu.edu.tw.

;; ADDITIONAL SECTION:
dns1.pme.nthu.edu.tw.   1D IN A         140.114.58.60
dns2.pme.nthu.edu.tw.   1D IN A         140.114.58.130

;; Total query time: 1 msec
;; FROM: mx to SERVER: dns1.nthu.edu.tw  140.114.64.10
;; MSG SIZE  sent: 33  rcvd: 103
```

   - dns1.pme.nthu.edu.tw NS 查到的 pme.nthu.edu.tw NS 也是 dns1.pme.nthu.edu.tw. 與 dns2.pme.nthu.edu.tw. 這兩筆。

```
# dig @dns1.pme.nthu.edu.tw pme.nthu.edu.tw ns
```

```
; <<>> DiG 8.3 <<>> @dns1.pme.nthu.edu.tw pme.nthu.edu.tw ns
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL:
2
;; QUERY SECTION:
;;      pme.nthu.edu.tw, type = NS, class = IN

;; ANSWER SECTION:
pme.nthu.edu.tw.        1D IN NS        dns2.pme.nthu.edu.tw.
pme.nthu.edu.tw.        1D IN NS        dns1.pme.nthu.edu.tw.

;; ADDITIONAL SECTION:
dns1.pme.nthu.edu.tw.   1D IN A         140.114.58.60
dns2.pme.nthu.edu.tw.   1D IN A         140.114.58.130

;; Total query time: 2 msec
;; FROM: mx to SERVER: dns1.pme.nthu.edu.tw  140.114.58.60
;; WHEN: Tue May 19 15:53:54 2009
;; MSG SIZE  sent: 33  rcvd: 103
```

TTL

每筆 DNS 記錄(record)其 TTL 由區域授權 NS 所指定，以本例而言，pme.nthu.edu.tw NS 指定 www.pme.nthu.edu.tw 的 TTL 為 1D (1 day)。

```
# dig @dns1.pme.nthu.edu.tw www.pme.nthu.edu.tw

; <<>> DiG 8.3 <<>> @dns1.pme.nthu.edu.tw www.pme.nthu.edu.tw
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      www.pme.nthu.edu.tw, type = A, class = IN

;; ANSWER SECTION:
www.pme.nthu.edu.tw.    1D IN A         140.114.57.163

;; AUTHORITY SECTION:
pme.nthu.edu.tw.        1D IN NS        dns2.pme.nthu.edu.tw.
pme.nthu.edu.tw.        1D IN NS        dns1.pme.nthu.edu.tw.

;; ADDITIONAL SECTION:
dns1.pme.nthu.edu.tw.   1D IN A         140.114.58.60
dns2.pme.nthu.edu.tw.   1D IN A         140.114.58.130
```

```
;; Total query time: 21 msec
;; FROM: mx to SERVER: dns1.pme.nthu.edu.tw  140.114.58.60
;; WHEN: Tue May 19 15:18:31 2009
;; MSG SIZE  sent: 37  rcvd: 123
```