DNS 技術實作

臺北市教育網路中心

基本設定練習：

狀況：

學校申請到的 Domain 是 ccjh.tp.edu.tw。學校共有五部機器，其中前兩部為 DNS Server，主機名稱與 IP 對應如下:

dns1.ccjh.tp.edu.tw (Master IP)
dns2.ccjh.tp.edu.tw (Slave IP)
www.ccjh.tp.edu.tw (163.21.252.10)
mail.ccjh.tp.edu.tw (163.21.252.11)
ftp.ccjh.tp.edu.tw (163.21.252.12)

學校申請到的 IP Address 為一個 Class C，資料為 163.21.252.0/24。

請與左右同學分別為 Master/Slave 關係，注意正反解皆須設定且一致。

注意：Master IP 請使用現在 PC 之 IP，Slave IP 則詢問左右同學。請注意 Master/Slave 設定上之語法差異。

步驟：

建立 named.conf

建立對應之 Zone Data File：Forward、Reverse、Root、LocalHost。

啟動 named

檢查 logfile，及檢測與 Debug

dns1 之 named.conf 內容範例：

```
options {
    directory "/var/named";
};

zone "." {
        type hint;
        file "named.ca";
};

zone "ccjh.tp.edu.tw" {
    type   master;
    file   "ccjh.tp.edu.tw.hosts";
};

zone "252.21.163.in-addr.arpa" {
    type   master;
    file   "163.21.252.rev";
};
zone “0.0.127.in-addr.arpa” { //…localhost 設定略};
```

定義 root dns Server 的檔案，可由
ftp://ftp.internic.net 取得或執行
dig @a.root-servers.net . ns > /var/named/named.ca

網域 ccjh.tp.edu.tw
為主控網域(Master)
正解檔(FQDN->IP)為 ccjh.tp.edu.tw.hosts

IP 211.72.100.X 之反解，IP 位址需要反寫為主控網域
反解檔(IP->FQDN)為 163.21.252.rev

正解檔 ccjh.tp.edu.tw.hosts 內容範例：

```
$TTL   4d
ccjh.tp.edu.tw.      IN    SOA       dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                      2003021901      ; Searil  number
                      24h             ; Refresh
                      2h              ; Retry
                      30d             ; Expire
                      1h )            ; Negative Cache
                      IN    NS        dns1.ccjh.tp.edu.tw.
                      IN    NS        dns2.ccjh.tp.edu.tw.
dns1                  IN    A       Master IP
dns2                  IN    A       Slave IP
mail                  IN    A       163.21.252.11
www                   IN    A       163.21.252.10
ftp                   IN    A       163.21.252.12
```

反解檔 163.21.252.rev 內容範例：

```
$TTL 38400
@                IN    SOA       dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                 2003122601  ; Searil  number
                 24h         ; Refresh
                 2h          ; Retry
                 1w          ; Expire
                 1h )        ; Negative Cache
                 IN    NS    dns1.ccjh.tp.edu.tw.
                 IN    NS    dns2.ccjh.tp.edu.tw.
<IP>             IN    PTR   dns1.ccjh.tp.edu.tw.
<IP>             IN    PTR   dns2.ccjh.tp.edu.tw.
10               IN    PTR   www. ccjh.tp.edu.tw.
11               IN    PTR   mail. ccjh.tp.edu.tw.
12               IN    PTR   ftp. ccjh.tp.edu.tw.
```

dns2 之 named.conf 內容範例：

```
options {
    directory "/var/named";
};

zone "." {
        type hint;
        file "named.ca";
};

zone "ccjh.tp.edu.tw" {
    type    slave;
```

masters 指出要跟那些 IP 做 Zone Transfer。

```
    masters {dns1 的 IP;} ;
    file   "ccjh.tp.edu.tw.zone";
};

zone   "163.21.252.in-addr.arpa"   {
    type   master;
    masters {dns1 的 IP;} ;
    file   "163.21.252.rev";
};
zone “0.0.127.in-addr.arpa” { //…localhost 設定略};
```

注意：正反解檔內容需互相對應。

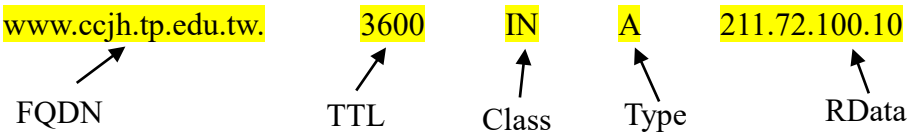
問題：

I. dns1 與 dns2 之正反解檔的建立與內容有何不同？

II. Masters 中如設定多個 IP，會有什麼樣的狀況發生？

以上都做好準備後，先進行檢測，可使用 BIND tool，像 nslookup 或 dig 來查詢。

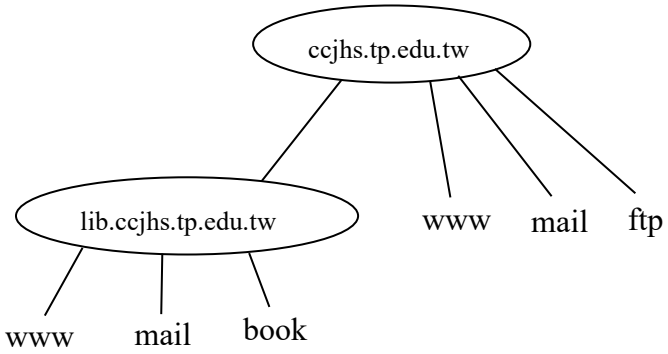
Resource Record 格式：



正反解子網域的分割與授權：

狀況：

學校中因圖書館電腦日益增多，為使圖書館在 Domain 的管理上有更多的自由與彈性，故在 ccjh.tp.edu.tw.這個 Domain 中，在分出一 SubDomain 名稱為 lib，也就是其 FQDN 為 lib.ccjh.tp.edu.tw.，圖書館有 Web Server，Mail Server 及 book(書目主機)，整體架構示意圖如下圖：



圖書館這三台主機的 IP Address 為 163.21.252.110、163.21.252.111 及 163.21.252.112。

練習一、代管模式：只作 SubDomain 的切割，但不真正授權給另一 Name Server 管理。

練習二、授權模式：將此 SubDomain 授權給另一 Name Server 管理，在本練習中請授權給 dns2 管理。

注意：兩種作法不同點

步驟：

作法一：dns1 修改對應之 Zone Data File

作法二：dns1 修改對應之 Zone Data File；dns2 修改 named.conf，並建立對應之 Zone Data File

重新啟動 named

檢查 logfile，及檢測與 Debug

作法一：

修改正解檔 ccjh.tp.edu.tw.hosts：

```
$TTL   4d
ccjh.tp.edu.tw.      IN    SOA      dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                     2003021901      ; Searil  number
                     24h             ; Refresh
                     2h              ; Retry
                     30d             ; Expire
                     1h )            ; Negative Cache
                     IN    NS        dns1.ccjh.tp.edu.tw.
                     IN    NS        dns2.ccjh.tp.edu.tw.
dns1                 IN    A      Master IP
dns2                 IN    A      Slave IP
mail                 IN    A      163.21.252.11
```

```
www             IN   A     163.21.252.10
ftp             IN   A     163.21.252.12
www.lib         IN   A     163.21.252.110
mail.lib        IN   A     163.21.252.111
book.lib        IN   A     163.21.252.112
```

圖書館這三行 RR(Resource Record)也可寫成

```
@ORIGIN    lib.ccjh.tp.edu.tw.
www             IN   A     163.21.252.110
mail            IN   A     163.21.252.111
book            IN   A     163.21.252.112
```

問題：正解檔中有關圖書館的資料還有那些種寫法，可達成同要需求？

此種設法，DNS 以集中的方式管理網域名稱下的所有資料，但當下層單位的主機有所變動時，需將需求反應給 DNS 的管理人員，請其調整 DNS 的資料。如果需求變化較多時，相對的造成 DNS Restart 的狀況及管理人員的負擔也會較多，故衡量狀況，有時我們會依其部門在 ccjh.tp.edu.tw. 的網域名稱下再建立 Sub-Domain，這些 Sub-Domain 由下層單位自行管控。

作法二：

dns1 修改正解檔 ccjh.tp.edu.tw.hosts：

```
$TTL   4d
ccjh.tp.edu.tw.     IN   SOA     dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                    2003021901      ; Searil  number
                    24h             ; Refresh
                    2h              ; Retry
                    30d             ; Expire
                    1h )            ; Negative Cache
                    IN   NS         dns1.ccjh.tp.edu.tw.
                    IN   NS         dns2.ccjh.tp.edu.tw.
dns1                IN   A      Master IP
dns2                IN   A      Slave IP
mail                IN   A      163.21.252.11
www                 IN   A      163.21.252.10
ftp                 IN   A      163.21.252.12
lib                 IN   NS     dns2.ccjh.tp.edu.tw.
```

圖書館這一行 RR(Resource Record)也可寫成

```
$ORIGIN    lib.ccjh.tp.edu.tw.
@                   IN   NS     dns2.ccjh.tp.edu.tw.
```

問題：dns1 正解檔中有關圖書館的資料還有那些種寫法，可達成同要需求？

dns2 要做的事：

修改 named.conf 檔：增加

```
zone   “lib.ccjh.tp.edu.tw” {
    type master;
    file "lib.ccjh.tp.edu.tw.hosts";
}
```

建立對應的 zone data file (lib.ccjh.tp.edu.tw.hosts)

```
$TTL   4d
@              IN      SOA     dns2.ccjh.tp.edu.tw.   sysadm.mail.lib.ccjh.tp.edu.tw. (
                   2003021901      ; Searil  number
                   24h             ; Refresh
                   2h              ; Retry
                   30d             ; Expire
                   1h )            ; Negative Cache
                   IN   NS         dns2.ccjh.tp.edu.tw.
www                IN   A      163.21.252.110
mail               IN   A      163.21.252.111
book               IN   A      163.21.252.112
```

問題：

dns2 有關圖書館的正解檔中：

1. @代表什麼意思？
2. NS Record 中定義 Name Server 為 dns2.ccjh.tp.edu.tw.，為何不需用 A Record 定義其 IP Address？什麼狀況下需要用 A Record 定義 IP Address？
3. 如要同時設定反解，要在那一台 Name Server 上設？
4. 如學校有另一組 Class C IP Address (211.72.101.0/24)，這組 Class C Address 要授權給圖書館全權管理與使用，圖書館有自己的 Name Server－ns1.lib.ccjh.tp.edu.tw 及 ns2.lib.ccjh.tp.edu.tw，在 dns1.ccjh.tp.edu.tw 及 ns1.lib.ccjh.tp.edu.tw 這兩台 Name Server 要如何設定？
5. 如全校共用一組 Class C IP Address(如原本之 211.72.100.0/24)，但要把 211.72.100.128/26(即 211.72.100.128~211.72.100.191)這 64 個 IP Address 授權給圖書館的Name Server管理，則dns1.ccjh.tp.edu.tw及ns1.lib.ccjh.tp.edu.tw這兩台Name Server 在反解的部份應如何設？

說明：

- A zone and a domain may share the same domain name but contain different nodes.
- 一個授權自行管理的 domain 會有一個 name server, 其所負責的區域稱做 zone, 但其範圍不含其授權管理的 subdomain
- Zone is bounded by delegation, it never includes delegated data.

E-Mail & DNS：

狀況：

學校有一台 Mail Server，其 FQDN 是 mail.ccjh.tp.edu.tw.，存放所有教職員的信箱。

1. 使用者的 E-Mail Address 在@後面是 mail.ccjh.tp.edu.tw，例如:tom@mail.ccjh.tp.edu.tw，在 DNS 上應如何設？
2. 如要使 E-Mail Address 儘量縮短，在@後面是 ccjh.tp.edu.tw，如 tom@ccjh.tp.edu.tw，DNS 上的設定為何？
3. 延續 2 的需求，但如校內有另一台電腦安裝電子郵件掃毒軟體(如 Interscan)，其 FQDN 為 scan.ccjh.tp.edu.tw.，要使郵件先經過其掃毒，再送至 mail.ccjh.tp.edu.tw，DNS 應如何設？
4. 如要使信件先經過市網心 smtp.tp.edu.tw 掃毒，再送至 mail.ccjh.tp.edu.tw，DNS 要如何設定？

步驟：

修改 ccjh.tp.edu.tw 所對應的 Zone Data File

重新啟動 named

1. **dns1 修改正解檔 ccjh.tp.edu.tw.hosts：**

```
$TTL   4d
ccjh.tp.edu.tw.     IN   SOA     dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                    2003021901     ; Searil  number
                    24h            ; Refresh
                    2h             ; Retry
                    30d            ; Expire
                    1h )           ; Negative Cache
                    IN   NS        dns1.ccjh.tp.edu.tw.
                    IN   NS        dns2.ccjh.tp.edu.tw.
mail                IN   MX   0    mail.ccjh.tp.edu.tw.
dns1                IN   A         Master IP
dns2                IN   A         Slave IP
mail                IN   A         163.21.252.11
www                 IN   A         163.21.252.10
ftp                 IN   A         163.21.252.12
```

mail IN MX 0 mail.ccjh.tp.edu.tw.這行也可寫成：

mail.ccjh.tp.edu.tw. IN MX 0 mail.ccjh.tp.edu.tw.

2. **dns1 修改正解檔 ccjh.tp.edu.tw.hosts：**

```
$TTL   4d
ccjh.tp.edu.tw.     IN   SOA     dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                    2003021901     ; Searil  number
                    24h            ; Refresh
                    2h             ; Retry
                    30d            ; Expire
                    1h )           ; Negative Cache
                    IN   NS        dns1.ccjh.tp.edu.tw.
```

```
                IN    NS        dns2.ccjh.tp.edu.tw.
                IN    MX   0    mail.ccjh.tp.edu.tw.
dns1            IN    A         Master IP
dns2            IN    A         Slave IP
mail            IN    A         163.21.252.11
www             IN    A         163.21.252.10
ftp             IN    A         163.21.252.12
```

在 Mail Exchanger(就是真正收信的 mail.ccjh.tp.edu.tw)之 Mail Server 程式(如 sendmail、Postfix)須設定將送往 ccjh.tp.edu.tw 把自己當成終點收進本機。

3. **dns1 修改正解檔 ccjh.tp.edu.tw.hosts：**

```
$TTL   4d
ccjh.tp.edu.tw.     IN    SOA       dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                    2003021901      ; Searil  number
                    24h             ; Refresh
                    2h              ; Retry
                    30d             ; Expire
                    1h )            ; Negative Cache
                    IN    NS        dns1.ccjh.tp.edu.tw.
                    IN    NS        dns2.ccjh.tp.edu.tw.
                    IN    MX   0    scan.ccjh.tp.edu.tw.
                    IN    MX   10   mail.ccjh.tp.edu.tw.
dns1                IN    A         Master IP
dns2                IN    A         Slave IP
mail                IN    A         163.21.252.11
www                 IN    A         163.21.252.10
ftp                 IN    A         163.21.252.12
```

在 scan.ccjh.tp.edu.tw 上須設定掃完毒的信不要再使用正常送信程序試著將信送往目的地，直接送給 mail.ccjh.tp.edu.tw。

問題：

I. 如果 scan.ccjh.tp.edu.tw 不設定掃完毒的信直接送給 mail.ccjh.tp.edu.tw 會有什麼狀況發生？

II. 設 IN MX 0 scan.ccjh.tp.edu.tw.，IN MX 10 mail.ccjh.tp.edu.tw 與只設 IN MX 0 scan.ccjh.tp.edu.tw 的差別在那裡？

4. **將信件的 Domain(ccjh.tp.edu.tw)、收信主機的 FQDN 及其 IP Address。**

dns1 修改正解檔 ccjh.tp.edu.tw.hosts：

```
$TTL   4d
ccjh.tp.edu.tw.     IN    SOA       dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                    2003021901      ; Searil  number
                    24h             ; Refresh
                    2h              ; Retry
                    30d             ; Expire
```

```
                1h )                ; Negative Cache
                IN    NS            dns1.ccjh.tp.edu.tw.
                IN    NS            dns2.ccjh.tp.edu.tw.
                IN    MX    0       smtp.tp.edu.tw.
                IN    MX    10      mail.ccjh.tp.edu.tw.
dns1            IN    A     Master IP
dns2            IN    A     Slave IP
mail            IN    A     163.21.252.11
www             IN    A     163.21.252.10
ftp             IN    A     163.21.252.12
```

問題、這個需求設定與 3 的有何差異？

問題：為何要設定 MX Record？

安全性設定：

狀況：

1. 限制只有校內的電腦才能使用學校的 DNS。
2. 限制只有特定的 DNS 可以跟 dns1 做 Zone Transfer，dns2 不允許任何電腦跟其做 Zone Transfer。

步驟：

修改 named.conf

```
options {
    directory "/var/named";
    allow-query { 163.21.252.0/24; } ;
    allow-transfer {dns2 的 IP;} ;
};
…….
zone "ccjh.tp.edu.tw" {
    type   master;
    file   "ccjh.tp.edu.tw.hosts";
    allow-query { any; };
};

zone "252.21.163.in-addr.arpa" {
    type   master;
    file   "163.21.252.rev";
    allow-query { any; };
};
```

問題：

I. 在 options 及 zone 中均設定 allow-query 的目的為何？

II. 如正解與反解兩個 Zone 要分別允許不同的 IP 做 Zone Transfer，要如何設？

III. 限制 Zone Transfer 的用意為何？

存取控制列表(ACL)：

狀況：

如果學校除了原本的 163.21.252.xxx 之外，又申請到兩組 Class C 之 IP Address，分別為 163.21.1.xxx 及 163.21.2.xxx。

在 named.conf 中使用 allow-query 限制校外電腦使用學校的 DNS，如何使 named.conf 設定更簡潔。

步驟：

更改 named.conf，在其中使用 acl 設定

重新啟動 named

修改 named.conf：

```
acl    ccjh_campus {
            163.21.252.0/24; 163.21.1.0/24; 163.21.2.0/24;
}
options {
    ……
            allow-query { ccjh_campus; } ;
}
```

acl 參數列表：

```
acl   acl_name    {
            IP;
            DN;
            path_name;
            CIDR;
            None;
            Any;
            Localhost;
            Localnets;
};
```

IP 位址 IP/[netmask]
網域名稱 *.twnic.net.tw
檔案名稱, 內存 ACL
IP 段163.21.249.128/25
沒有任何 IP
任何 IP
localhost (127.0.0.1)
網卡的 IP/Netmask (即相連的網路)

Logging 的設定：

狀況：

將所有電腦到學校 DNS Query 的資料都記錄下來，同時記錄所有認可與不認可的 Query。

步驟：

更改 named.conf，在其中使用 acl 設定

重新啟動 named

在 named.conf 中加入：

```
logging {
        channel SEC_log {
                file "/var/log/dns-sec.log" versions       3 size 1m;
                severity info;
                print-severity    yes;
                print-time          yes;
        };
        channel QUERY_log {
                file "/var/log/dns-query.log" versions     3 size 1m;
                severity info;
                print-severity    yes;
                print-time          yes;
        };
        category security { SEC_log; };
        category queries { QUERY_log; };
};
```

dns-query.log 範例：

```
Feb 14 16:46:14.386 info: client 139.175.252.16#2059: query: ms.slhs.tp.edu.tw IN A
Feb 14 16:46:24.354 info: client 203.72.185.10#1491: query: seed.net.tw IN MX
Feb 14 16:46:31.442 info: client 172.16.1.202#2962: query: www.symantec.com IN A
Feb 14 16:46:32.794 info: client 168.95.192.148#32805: query: proxy.slhs.tp.edu.tw IN A
Feb 14 16:46:39.917 info: client 203.72.185.102#39886: query: ms.slhs.tp.edu.tw IN A
Feb 14 16:46:39.919 info: client 203.72.185.10#1493: query: 102.185.72.203.in-addr.arpa IN PTR
Feb 14 16:46:39.920 info: client 203.72.185.10#1494: query: smtp.slhs.tp.edu.tw IN A
Feb 14 16:46:48.149 info: client 203.72.185.102#39886: query: ms.slhs.tp.edu.tw IN A
Feb 14 16:46:48.151 info: client 203.72.185.10#1495: query: 102.185.72.203.in-addr.arpa IN PTR
Feb 14 16:46:48.152 info: client 203.72.185.10#1496: query: smtp.slhs.tp.edu.tw IN A
Feb 14 16:46:55.600 info: client 203.72.185.1#2305: query: 42.81.216.61.in-addr.arpa IN PTR
Feb 14 16:46:59.332 info: client 203.72.185.1#2306: query: 42.81.216.61.in-addr.arpa IN PTR
Feb 14 16:46:59.334 info: client 203.72.185.1#2307: query: 61-216-81-42.HINET-IP.hinet.net IN A
Feb 14 16:47:07.891 info: client 140.122.53.102#1026: query: microsoft.com IN A
```

dns-sec.log 範例：

```
Feb 11 00:42:00.012 info: client 61.55.138.141#2562: query (cache) denied
Feb 11 00:42:00.224 info: client 61.55.138.141#2562: query (cache) denied
Feb 11 00:42:00.983 info: client 61.55.138.141#2562: query (cache) denied
Feb 11 00:43:31.480 error: client 203.72.187.234#3447: update 'slhs.tp.edu.tw/IN' denied
```

Feb 11 00:43:31.495 error: client 203.72.187.234#3452: update '187.72.203.in-addr.arpa/IN' denied
Feb 14 16:23:12.182 error: client 203.72.187.234#15941: update 'slhs.tp.edu.tw/IN' denied
Feb 14 16:23:12.199 error: client 203.72.187.234#15947: update 'slhs.tp.edu.tw/IN' denied
Feb 14 16:23:12.215 error: client 203.72.187.234#15953: update 'slhs.tp.edu.tw/IN' denied
Feb 14 16:23:12.232 error: client 203.72.187.234#15959: update 'slhs.tp.edu.tw/IN' denied
Feb 14 16:26:31.447 info: client 172.16.1.202#2958: query (cache) denied
Feb 14 16:31:31.445 info: client 172.16.1.202#2959: query (cache) denied
Feb 14 16:36:31.443 info: client 172.16.1.202#2960: query (cache) denied
Feb 14 16:41:31.443 info: client 172.16.1.202#2961: query (cache) denied

dns-lamer.log 範例：

Feb 14 16:27:56.979 info: lame server resolving 'settv.com.tw' (in 'settv.com.tw'?): 61.63.90.100#53
Feb 14 16:27:56.980 info: lame server resolving 'settv.com.tw' (in 'settv.com.tw'?): 61.63.90.100#53

lamer Server 說明：

1.先找出負責 com.tw 的 name server 有那些：

root@dns [4:51pm] ~ > *dig com.tw ns*

……

;; QUESTION SECTION:

;com.tw. IN NS

;; ANSWER SECTION:

com.tw.	518400	IN	NS	ns2.cuhk.edu.hk.
com.tw.	518400	IN	NS	a.twnic.net.tw.
com.tw.	518400	IN	NS	b.twnic.net.tw.
com.tw.	518400	IN	NS	c.twnic.net.tw.
com.tw.	518400	IN	NS	d.twnic.net.tw.
com.tw.	518400	IN	NS	e.twnic.net.tw.

;; ADDITIONAL SECTION:

a.twnic.net.tw.	46441	IN	A	192.83.166.9
a.twnic.net.tw.	29448	IN	AAAA	2001:288:1:1002:2e0:18ff:fe77:f174
b.twnic.net.tw.	47158	IN	A	192.72.81.200
c.twnic.net.tw.	47158	IN	A	168.95.192.10
d.twnic.net.tw.	47213	IN	A	210.17.9.229
d.twnic.net.tw.	32445	IN	AAAA	2001:c50:ffff:1:2e0:18ff:fe95:b22f
e.twnic.net.tw.	47204	IN	A	211.79.207.25
ns2.cuhk.edu.hk.	90134	IN	A	137.189.6.21

2.到 a.twnic.net.tw 問負責 settv.com.tw 的 name server 有那些：

root@dns [4:53pm] ~ > ***dig @192.83.166.9 settv.com.tw ns +norec***

…….

;; QUESTION SECTION:

;settv.com.tw. IN NS

;; AUTHORITY SECTION:

settv.com.tw.	86400	IN	NS	setweb.settv.com.tw.

```
settv.com.tw.           86400   IN      NS      sanlih.com.tw.

;; ADDITIONAL SECTION:
sanlih.com.tw.          86400   IN      A       61.63.90.100
setweb.settv.com.tw.    86400   IN      A       61.63.90.1
```

可以看出 settv.com.tw 在上層的 DNS 上註冊有兩台 name server，分別為 sanlih.com.tw (61.63.90.100) 及 setweb.settv.com.tw(61.63.90.1)

3.到 sanlih.com.tw(61.63.90.100)查負責 settv.com.tw 的 name server 有那些？

root@dns [4:56pm] ~ > ***dig @61.63.90.100 settv.com.tw ns +norec***

```
……
;; QUESTION SECTION:
;settv.com.tw.                  IN      NS

;; ANSWER SECTION:
settv.com.tw.           22338   IN      NS      setweb.settv.com.tw.

;; ADDITIONAL SECTION:
setweb.settv.com.tw.    75099   IN      A       61.63.90.1
```

發現負責 settv.com.tw 的 name server 只有 setweb.settv.com.tw.(61.63.90.1)。同樣的到 setweb.settv.com.tw (61.63.90.1) 查也得到同樣的結果。

root@dns [DING!] ~ > ***dig @61.63.90.1 settv.com.tw ns +norec***

```
……
;; QUESTION SECTION:
;settv.com.tw.                  IN      NS

;; ANSWER SECTION:
settv.com.tw.           38400   IN      NS      setweb.settv.com.tw.

;; ADDITIONAL SECTION:
setweb.settv.com.tw.    38400   IN      A       61.63.90.1
```

本身 DNS 所設定的 NS Record 與上層註冊的資料不一致。而且 sanlih.com.tw(61.63.90.100) 並不負責 settv.com.tw 這個 Domain。

Log 的類別(category)：

default	指定以外的所有訊息
cname	CNAME 的錯誤
lame-servers	不良的委任設定
load	載入 zone file 時的訊息
notify	變更通知
os	作業系統相關問題
packet	收送之封包,需指向檔案
panic	引起 dns 關閉的原因

parser	檢查組態檔的語法
statistics	DNS 活動的定時報告
security	被認可或不被認可的請求
update	動態更新事件
xfer-in	zone-transfer in

問題：

1. 為何要做 Log？
2. 前面列出的 log 類別(category)中，那些 BIND 9 已不支援？

BIND9 新增功能($GENERATE)：

狀況：

電腦教室中有 50 台電腦，IP Address 從 163.21.252.51 到 163.21.252.100，Domain Name 分別為 pc51.ccjh.tp.edu.tw、pc52.ccjh.tp.edu.tw…..pc100.ccjh.tp.edu.tw，全部都要在 DNS 註冊。

步驟：

修改對應之正解檔
修改對應之反解檔
重新啟動 named

作法一、

在正解檔(ccjh.tp.edu.tw.hosts)中加入：

```
pc51        IN      A       163.21.252.51
pc52        IN      A       163.21.252.52
…….
Pc100       IN      A       163.21.252.100
```

在反解檔(211.72.100.rev)中加入：

```
51          IN      PTR     pc51.ccjh.tp.edu.tw.
52          IN      PTR     pc52.ccjh.tp.edu.tw.
…….
100         IN      PTR     pc100.ccjh.tp.edu.tw.
```

作法二、

在正解檔(ccjh.tp.edu.tw.hosts)中加入：

```
$GENERATE   51-100    pc$    A    163.21.252.$
```

在反解檔(163.21.252.rev)中加入：

```
$GENERATE   51-100    $      PTR    pc$.ccjh.tp.edu.tw.
```

注意：

使用$GENERATE 時，Class IN 是不可寫的。例如：
$GENERATE 51-100 pc$ **IN** A 163.21.252.$ 是不正確的寫法。

問題：

如果 IP 是從 163.21.252.101 到 163.21.252.151，是否也可用一行$GENERATE 指令完成？

使用 rndc：

狀況：

設定 rndc，以便使用 rndc 對 named 下各種指令，如 reload 所有 zone data 及 configuration，亦可進一步控制別台主機上的 BIND。

步驟：

產生 rndc.conf 於/usr/local/etc 中
更改 named.conf 加入相關設定
重新啟動 named

1. 使用 rndc-confgen 產生 rndc.conf：

執行 rndc-confgen -r keyboard > rndc.conf (或用 rndc-confgen > rndc.conf)

```
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "FryPy+SFDPtWh2VxBTldyw==";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-md5;
#       secret  "FryPy+SFDPtWh2VxBTldyw==";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

2. 在 named.conf 中加入：

```
key "rndc-key" {
        algorithm hmac-md5;
        secret  "FryPy+SFDPtWh2VxBTldyw==";
};

controls {
        inet 127.0.0.1 port 953
                allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

rndc 指令格式與參數說明：

Usage: rndc [-c config] [-s server] [-p port] [-k key-file] [-y key] [-V] command

command is one of the following:

reload	Reload configuration file and zones.
reload zone [class [view]]	Reload a single zone.
refresh zone [class [view]]	Schedule immediate maintenance for a zone.
reconfig	Reload configuration file and new zones only.
stats	Write server statistics to the statistics file.
querylog	Toggle query logging.
dumpdb	Dump cache(s) to the dump file (named_dump.db).
stop	Save pending updates to master files and stop the server.
halt	Stop the server without saving pending updates.
trace	Increment debugging level by one.
trace level	Change the debugging level.
notrace	Set debugging level to 0.
flush	Flushes all of the server's caches.
flush [view]	Flushes the server's cache for a view.
status	Display status of the server.
*restart	Restart the server.

* == not yet implemented
Version: 9.2.3

問題：

是否可以使用 rndc 來控制其他電腦上的 BIND？如果可以，有些什麼步驟要做？

BIND9 新增功能(view)：

狀況：

在 dns1 上設定，使 dns2 到 dns1 查 ccjh.tp.edu.tw 的資料時，dns1 回應 private IP address(192.168.1.xxx)，但 dns1 本身查時，則查到原本合法的 IP Address(163.21.252.xxx)。

步驟：

修改 named.conf
建立新的正反解 Zone Data File
重新啟動 named

1. 修改 named.conf，加入：

```
view   "view_in" {
            match-clients {dns2 的 IP Address; } ;
            recursion   yes ;
            zone "ccjh.tp.edu.tw" {
                type master ;
                file   "ccjh.tp.edu.tw.dns2" ;
            } ;
            zone "1.168.192.in-addr.arpa" {
                type   master;
                file   "192.168.1.rev";
            };
};
view "view_out" {
            match-clients {any;} ;
            recursion no ;
            zone   "ccjh.tp.edu.tw" {
                type master ;
                file   "ccjh.tp.edu.tw.hosts" ;
            } ;
            zone "252.21.163.in-addr.arpa" {
                type   master;
                file   "163.21.252.rev";
            };
};
```

2. **建立新的正反解 Zone Data File，ccjh.tp.edu.tw.dns2 及 192.168.1.rev：**

正解檔(ccjh.tp.edu.tw.dns2)：

```
$TTL   4d
ccjh.tp.edu.tw.      IN    SOA       dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                      2003021901      ; Searil   number
                      24h             ; Refresh
                      2h              ; Retry
                      30d             ; Expire
                      1h )            ; Negative Cache
                      IN    NS        dns1.ccjh.tp.edu.tw.
dns1                  IN    A         Master IP
```

```
mail            IN    A       192.168.1.11
www             IN    A       192.168.1.10
ftp             IN    A       192.168.1.12
```

反解檔(192.168.1.rev)：

```
$TTL 38400
@               IN    SOA     dns1.ccjh.tp.edu.tw.   sysadm.mail.ccjh.tp.edu.tw. (
                2003122601    ; Searil  number
                24h           ; Refresh
                2h            ; Retry
                1w            ; Expire
                1h )          ; Negative Cache
                IN    NS      dns1.ccjh.tp.edu.tw.
10              IN    PTR     www. ccjh.tp.edu.tw.
11              IN    PTR     mail. ccjh.tp.edu.tw.
12              IN    PTR     ftp. ccjh.tp.edu.tw.
```

注意：

I. 如果學校校內使用 Private IP Address，要使校外電腦查詢學校 Domain Name 資料時可查到學校合法的 IP Address；然而校內電腦查詢同一 Domain Name 時，會查到 Private IP Address，此種需求可使用兩台 Name Server，一台供校外查，一台供校內查；但如果只使用一台 Name Server，怎可使用 BIND 9 的 view 設定。

II. 在 named.conf 中，所有 zone 敘述都要包含在 view 敘述中。

III. 每一個 view 都有一行 match-clients，決定何種 address 要採用此 view 的設定，view 在 named.conf 中採 first match，因此 view 在 named.conf 中排列的順序很重要。

Serial Number 錯誤修正：

狀況：

學校只有一台 Name Server，請市網 dns2.tp.edu.tw 幫忙作第二台 Name Server。在某次修改 Zone Data File 時不小心設定了錯誤的 Serial Number(200402160101)，但並沒有及時發現，隔了幾天才發現錯誤，應如何修正 Serial Number 使市網 dns2.tp.edu.tw 所 Cache 的資料與學校 Name Server 的資料確保一致。

注意：

Serial Number 為一 2^{32} 的整數，其中有一半比目前的 Serial Number 小，其餘的比目前的 Serial Number 大。

方法一、

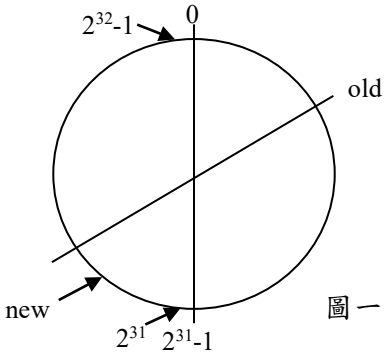
1. 將錯誤的 Serial Number 修正。
2. 請市網工作人員將 dns2.tp.edu.tw 上對應的 Cache Zone Data File 刪除，再重新啟動 dns2.tp.edu.tw 的 named。

方法二、(如因故無法將 dns2.tp.edu.tw 上對應的 Cache Zone Data File 刪除)

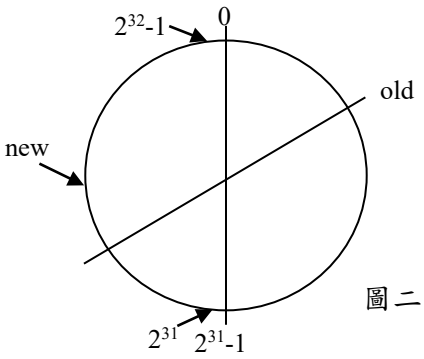
依照下列 algorithm 步驟修正：

1. 先用 nslookup 或 dig 找出目前真正的 Serial Number。
2. 假設 old 代表錯誤的 Serial Number，new 代表修正後的 Serial Number。

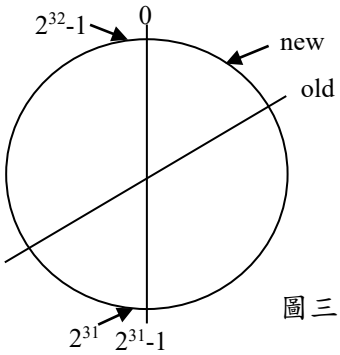
```
If  old  <  new  Then  {
    If  (new – old)  <  2^31  Then  {  (圖一)
        設定 new 為新的 Serial Number
    }
    Else  {  (圖二)
        先設定 Serial Number 為  old + 2^31 - 1，
        等 slave name server 更新後，再設定 Serial Number 為  new
    }
}
Else {
    If  (old + 2^31 – 1)  <  2^32 – 1  Then  {  (圖三)
        先設定 Serial Number 為  old + 2^31 - 1，
        等 slave name server 更新後，再設定 Serial Number 為  new
    }
    Else If  (old + 2^31 – 1) MOD 2^32  <  new  Then  {  (圖四)
        先設定 Serial Number 為  old + 2^31 - 1，
        等 slave name server 更新後，再設定 Serial Number 為  new
    Else  {  (圖五)
        設定 new 為新的 Serial Number
    }
}
```



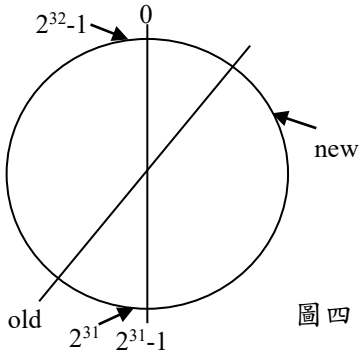
圖一



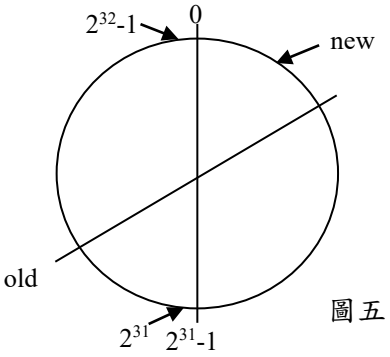
圖二



圖三



圖四



圖五

問題：

1. 如果 Serial Number 弄亂後，直接改回正確的會有什麼樣的結果。
2. 為何看 Zone Data File 中之 Serial Number 是不正確的？要如何才能找出目前真正的 Serial Number？

DEBUG：

下列狀況設定上有何問題？會產生什麼樣的狀況？

狀況一、

市網設定：

```
$ORIGIN    ccjh.tp.edu.tw.
@          IN   NS    web.ccjh.tp.edu.tw.
web        IN   A     163.21.252.1
```

學校端設定：

```
@          IN   SOA   ……
……
           IN   NS    dns.ccjh.tp.edu.tw.
dns1       IN   A     163.21.252.1
Web        IN   CNAME dns
```

狀況二、

市網設定：

```
$ORIGIN    ccjh.tp.edu.tw.
@          IN   NS    web.ccjh.tp.edu.tw.
web        IN   A     163.21.252.1
```

學校端設定：

```
@          IN   SOA   ……
……
           IN   NS    dns.ccjh.tp.edu.tw.
dns1       IN   A     163.21.252.1
```

DNS 與網路安全

DNS 的安全性在整體的網路安全中佔有相當重要的地位，而卻常常被忽略，這除了因為不熟悉外，主要針對 DNS 的攻擊並不多見，但其影響卻超出一般人想像。

以下引用幾條新聞訊息:

http://www.sinica.edu.tw/info/security/news-%C0b%AB%C8%A7%F0%C0%BB%C2%EA%A9w.info%BA%F4%B0%EC%A8t%B2%CE.htm

駭客攻擊鎖定.info 網域系統

上周網域名管理公司 UltraDNS 遭一波網際網路垃圾資訊轟炸，造成掛在.info 和其他網域名稱上的網站伺服器癱瘓，管理員為維護系統正常運作而疲於奔命。

UltraDNS 執行長 Ben Petro 說，上周四（11 月 21 日）早晨，在網路使用量最大的四小時內，這波攻擊每秒鐘向連上網際網路的各個裝置發出將近 200 萬則查詢訊息，是正常量的數倍之多，導致 UltraDNS 的系統難以消受。

「這是我們經歷過規模最大的一次攻擊，」Petro 說。他強調，這場攻擊並未影響到該公司核心的網域名系統（domain name system，簡稱 DNS）服務，但系統管理員必須迅速行動，請提供 UltraDNS 網路連線的骨幹網際網路公司攔阻那些垃圾訊息。「從網路管理的觀點來看，這的確讓我們緊張萬分，」他說。

將近一個月前，也出現類似鎖定 DNS 根伺服器的攻擊。所謂 DNS 根伺服器（DNS root servers）指的是一種資料庫，內含電腦維持頂層網域所需的重要資料。這些網域的作用如同網際網路版的電話簿白頁（white pages），將網域名稱（例如 www.cnet.com）與數據形式的網際網路位址逐一配對。

Petro 說，有關當局可能正著手調查此案。

但調查人員要找出發動攻擊者的位置，談何容易。用垃圾訊息灌爆網路，也就是眾所周知的分散式阻斷服務攻擊（distributed denial-of-service attacks），通常都是駭客用偽造的來源位址、透過事前即侵入的伺服器所發動。運用這種雙重的間接手法，使得元兇難以追查。

但 Petro 說，揪出攻擊者的重要性與日俱增，因為最近網際網路攻擊的趨勢已改變，已從原先鎖定零星的公司，轉變成瞄準網際網路基礎設施本身發動攻擊。

「當你癱瘓亞馬遜網站時，傷害的只是亞馬遜，」他說。「但是當你擊垮.com、.org 和 .net 時，影響的是一國的國內生產毛額（GDP），受害的會是全國的經濟。」

UltraDNS 是網際網路協會（Internet Society）的會員，是.org 網域名的主要 DNS 供應者。UltraDNS 另外也提供 .info 網域，以及愛爾蘭、盧森堡和挪威的頂層網域及其他九種網域。

「現實是，網路攻擊規模愈來愈大、愈演愈烈而且愈來愈快速，」Petro 說。「如同恐怖攻擊，你不知攻擊行動何時發生、如何發生。除非我們密切關注這些攻擊事件，而且追查出源頭，我們都可能淪為受害者。」

(http://www.secretchina.com/news/articles/2/10/23/27110b.html)

全球互聯網系統核心 21 日遭規模最大攻擊

2002 年 10 月 23 日 星期三

美國官員及電腦專家表示，掌管全球網際網路交通的十三座根名稱伺服器（root server）二十一日晚間曾同時遭不明人士攻擊達一小時，目的顯然是要癱瘓全球網路，這是網際網路創立以來所遭受規模最大、也最複雜的網路攻擊行動。

據自由時報綜合二十二日外電報導，美國加州「網路軟體協會」負責人維克西表示，

上述攻擊行動是在美國東岸時間二十一日下午五時（台北二十二日清晨五時）左右開始，歷時約一小時，網際網路領域名稱系統（ＤＮＳ）的十三座根名稱伺服器同時遭人以「分散式阻斷服務」方式攻擊，造成部份網路交通受阻，但一般網路使用者並未察覺有異。

一位電腦專家指出，由於二十二日下午數個網站也曾遭到類似的攻擊，他猜測，這很可能是同一票人尋找新目標攻擊作樂。

美國聯邦調查局（ＦＢＩ）發言人指出，該局轄下的全國基礎建設保護中心已得知此事，並展開調查行動。美國官員也證實，十三座根名稱伺服器中，有九座在攻擊期間無法正常運作，但在電腦專家立即採取防禦措施，以及攻擊歹徒忽然停手後，網路交通隨即恢復正常。

參與搶救的匿名電腦專家還透露，他們曾與白宮國土安全辦公室和布希總統的關鍵基礎建設保護署合作。

網路領域名稱系統可讓各電腦網路系統在使用者鍵入的文字名稱以及用數字代碼來表示的網址之間進行轉換，但仍必須仰賴根伺服器來提供網址資訊，因此這十三座分布在全球各地，由美國政府機關、各大學、企業和私人組織負責運作的根伺服器一直都被網路安全專家視為網際網路最大的弱點，很有可能在網路遭人惡意攻擊時當機。

據維克西指出，網路根伺服器過去也曾遭到攻擊，但十三座伺服器同時遭到攻擊則相當罕見，但此次攻擊行動也證明瞭網路無法輕易被阻斷，因為網際網路設計的原旨就是要繞過障礙。

其他電腦專家則表示，此次攻擊未對網路造成重大影響，主因是許多網路服務供應者及大型企業或組織都會儲存或「快取」最受歡迎的網路資訊分類目錄，而不必全部仰賴根伺服器進行轉換的緣故。雖然理論上網路可在僅有一座根伺服器的情況下運作，但假若四座以上的根伺服器同時當機時間過長，網路運作的速度就會明顯減慢.

http://www.fanqiang.com/a5/b1/20010520/090400150_b.html

從 DNS 入侵機器的過程一次被 DNS 攻擊後的分析

http://www.fanqiang.com (2001-05-20 09:04:00) BY XUNDI

原文作者：lance@spitzner.net

這篇文章是關於被 DNS 攻擊後的系統分析，通過這個分析可以了解攻擊者的行為，能很好的了解怎樣攻擊，攻擊後做什麼等各種行為，有助你更好的維護系統。

背景

此文資訊與 honeypot--http://project.honeynet.org/ 有關的，Honeypot 在 REDHAT 上是一個預設的服務裝設，其字面意思是蜜缸，呵呵，即使說用來引誘某些...的一個陷阱，呵呵。下面分析的所有 IP 位址用戶帳號和 Keyin 的資訊是真實的，除了密碼資訊，這樣是為了更直接的了解整個過程。所有 SNIFF 資訊是通過 SNORT 格式展現的；http://www.snort.org/的 SNORT 是一個常用的嗅探器，對於偵測系統入侵分析來說是一個不錯的工具，我使用在 http://www.whitehats.com/的 MAX VISION 的 IDS 簽字。

攻擊行為

在四月 26 號，snort 提醒我其中的一個系統正受到一個'noop'攻擊，資訊包裝載包含 noops 的資訊，在此情況下，SNORT 探測到攻擊和記錄了警告資訊到/var/log/messages 文件中（使用 http://www.enteract.com/~lspitz/swatch.html--swatch 來監控），注意這文中 172.16.1.107 的 IP 位址是含有 honeypot 的機器，其他的位址是 black-hat(黑帽子）使用的 IP 位址。

Apr 26 06:43:05 lisa snort[6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

我的 honeypots 接受無數探測，掃描和查詢，而且下面的一個警告資訊使我注意到其中一個系統可能被破壞，下面的系統 LOG 資訊指示攻擊者正開始了一個連接和 LOGIN 了系統：

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user twin by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user hantu by twin(uid=506)

從上面的情況可以看到，入侵者已經獲得超級用戶權利和控制了整個系統，但這是怎樣完成的呢，我們下面開始分析：

分析

當分析一攻擊的時候，最好的位置是在開始端，即攻擊者是從哪開始的，攻擊者一般開始是收集系統資訊，可以讓他獲得系統所存在的漏洞，如果你的系統被破壞，這就表明攻擊者不是第一次與你的系統通信了，大多數攻擊者必須通過對你系統的連接獲得初始化的資訊。

所以我們從最開始的資訊收集開始，從第一條資訊可以知道攻擊初於 53 連接埠，這表示在我們系統上發動了一個 DNS 攻擊，所以我通過我的 snort alerts--http://www.enteract.com/~lspitz/probed.txt 來發現一些 DNS 可能的資訊探測，我們發現一 DNS 版本查詢探測的資訊：

Apr 25 02:08:07 lisa snort[5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53
Apr 25 02:08:07 lisa snort[5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

注意，這個探測日期是 4 月 25 日，我們系統被攻擊是在 4 月 26 號，系統是在被探測後的一天被入侵的，所以我猜測攻擊者是使用一些掃描器掃描出一些關於 DNS 漏洞的資訊，掃描以後，攻擊者查看掃描結果，獲得系統漏洞資訊，然後啟用他們的 EXPLOIT。
這樣我們可以得到如下結論：在 4 月 25 號被偵測後，後一天被侵入，通過我們的 IDS 警告，我們獲知我們是被 DNS 漏洞攻擊。

THE EXPLOIT：
類似於大多數商業 IDS 系統，snort 可以顯示我們所有 IP 資訊包裝載數據，我們就使用這功能來分析 EXPLOIT，這個 EXPLOIT 資訊可以從 snort 的 LOG 記錄獲得（存儲在 tcpdump 兩進制格式）。我查詢 snort 的 LOG 記錄並開始分析攻擊開始時候的資訊包，我沒有把資訊限制在僅查詢主機 63.336.81.13，主要是因為攻擊者使用三個
不同系統來執行這個 EXPLOIT，這個 EXPLOIT 的目標是在遠端主機上獲得 ROOT SHELL，一旦攻擊者獲得 ROOT SHELL，他們可以以 ROOT 身份執行所有命令，還通常

會在/etc/passwd 和/etc/shadow 文件中增加帳號，下面的獲得 ROOT SHELL 後執行的一些命令：

```
cd /; uname -a; pwd; id;
Linux apollo.uicmba.edu 2.2.5-15 #1 Mon Apr 19 22:21:09 EDT 1999 i586 unknown
/
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
echo "twin::506:506::/home/twin:/bin/bash" >> /etc/passwd
echo "twin:w3nT2H0b6AjM2:::::::" >> /etc/shadow

echo "hantu::0:0::/:/bin/bash" >> /etc/passwd
echo "hantu:w3nT2H0b6AjM2:::::::" >> /etc/shadow
```

從上面可以知道，攻擊者執行了 uname -a 查詢了系統，和 PWD 查詢目前工作目錄，和 ID 查看 UID，並增加了 twin 和 hantu 兩個帳號，使用了相同的密碼，必須注意，twin 使用了 UID 為 506，而 hantu 使用了 UID 為 0（另一方面 hantu 是印度尼西亞語言中的鬼魂的意思），要知道，大多數系統中不允許 UID 為 0 的帳號遠端 TELNET，所以起建立了一個可以遠端 TELNET 的帳號，並建立了以後可以 SU 到 ROOT 的帳號。在 90 秒內攻擊者利用了 EXPLOIT 程式進入系統，並獲得 ROOT 權利（可以通過下面的 LOG 記錄），

```
Apr 26 06:43:05 lisa snort[6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user twin by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user hantu by
twin(uid=506)
```

在 5 月 9 號，10：45 早上，攻擊者從 24.7.85.192 再次 TELNET 機器，注意其設定了 VT9111 不認進入了系統：

snort 的相應網址：http://www.snort.org/

上述三篇轉載文章我們可以看出 DNS 安全的重要性，而愈處上層就需更考慮到安全性，如果 .tw 的 Root Server 不安全，那全台灣的 DNS 可能都會發生問題，即便是全台的網路會出問題。而若 ISP 的 DNS 不安全，因其提供眾多的用戶查詢，亦可能產生重大的問題。一般公司行號的 DNS 雖然不會造成如此大事件，但是依然可能對公司造大重大傷害，故安全性問題不可不慎。

BIND 安全與版本息息相關，詳細對應關係請參考 http://www.isc.org/products/BIND/bind-security.html

SPOF(Single Point of Failure)之問題

SPOF 即是只有一部 DNS 之問題，這種狀況其實不符合 InterNIC 的規定，以 TWNIC 而言，做 DNS 指定時，都要您填寫兩部以上之資料，其原因:

容錯：若您僅有一部 DNS 主機時，相信很多人都有經驗的是該主機失效後，網路的眾多功能也會跟著失效（Web/Mail…），但若您有兩部以上的 DNS 主機則大大降低了這樣的可能性。若您的 DNS 分佈在不同的 ISP 網段，更可降低網路斷線所造成的眾多問題。

負載平衡：若您設定了兩部以上的 DNS 主機，當有人連接您的網站前，其接受 DNS 查詢乃是兩台主機輪流運作(輪詢，Round-Robin)。在這樣的運作機制下讓您的系統可以更穩定。

系統安全：目前網路上有著許多可以針對 DNS 作攻擊的程式，若您擁有兩台以上的主機，可降低許多來自於攻擊的危險（至少增加了一倍的安全性，其中不同的

主機尚可運作不同的作業系統)。因為絕大多數的 DNS 查詢或攻擊皆是使用 UDP 協定(User Datagram Protocol)，在攻擊發生時較不容易被查覺。

SPOF 問題最有名案例即是 2001 年時，微軟的四部 DNS 主機皆擺在同一個 LAN 之下，而當這個 LAN 對外的 Router 被攻垮後，所有的 DNS 即失去作用。進而，對許多人而言，微軟好像從網路上消失一般。所以，若您的單位對安全議題較重視，不能忽略失去 DNS 對您網路的影響。

遠端溢位問題/拒絕服務存取

遠端溢位(Remote buffer overflow) 是多數系統不能避免的安全漏洞，而 BIND 某些版本亦存在此一問題，您可參考 http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl 網址，於 Vendor 處選擇 ISC ，則可列出 BIND 所有的系統問題，其中我們選擇 TSIG Vuln，這是一個可以遠端溢位的漏洞，於 http://www.securityfocus.com/data/vulnerabilities/exploits/tsig.c 可以取得溢位的範例程式。由 tsig 的漏洞公告中，我們知道這個問題可能被取得系統權限，而受影響的版本幾乎包括了 8.2.3(不含)以下所有的版本。由此可見，任何人其實都可以很容易取得這一類資源。其中最有名的即是當年度之 Lion Worm，以類似 Code Red 型式之 Worm 在網路上尋找 DNS 主機並攻擊入侵，最後將 /etc/passwd /etc/shadow 檔寄給作者。

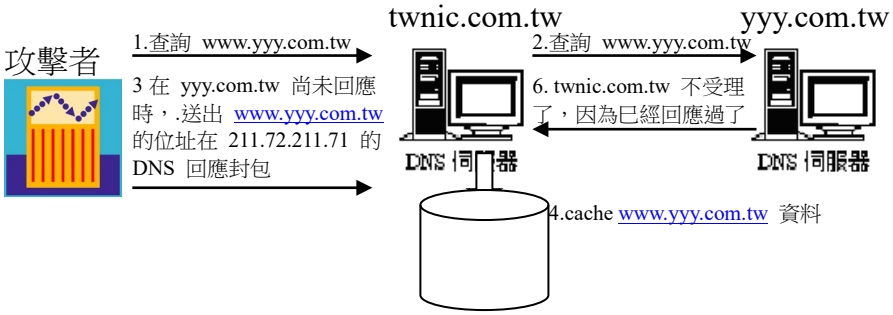
拒絕服務存取的攻擊目前已不可勝數，其目的多不在於入侵系統，而是癱瘓整個網路系統，這個問題目前幾乎是無解，僅能以被動的方式來防禦，同樣的在 http://www.securityfocus.com/ cgi-bin/sfonline/vulns.pl 的資料上您也可以看到許多這類的資訊。

基本上亦建議，若環境允許，您不要將所有的的服務皆擺在同一部主機，因為一旦某一服務發生問題(如 Mail/Web/DNS/…)，其他服務可能皆受影響，對您單位的網路運作影響甚大。

上述兩種網安的狀況屢見不鮮，不過這類攻擊因為特徵明顯，多少可由入侵偵測系統(IDS)或防火牆所發現，但 DNS 欺騙則可能較不容易被偵測到。

欺騙手法一

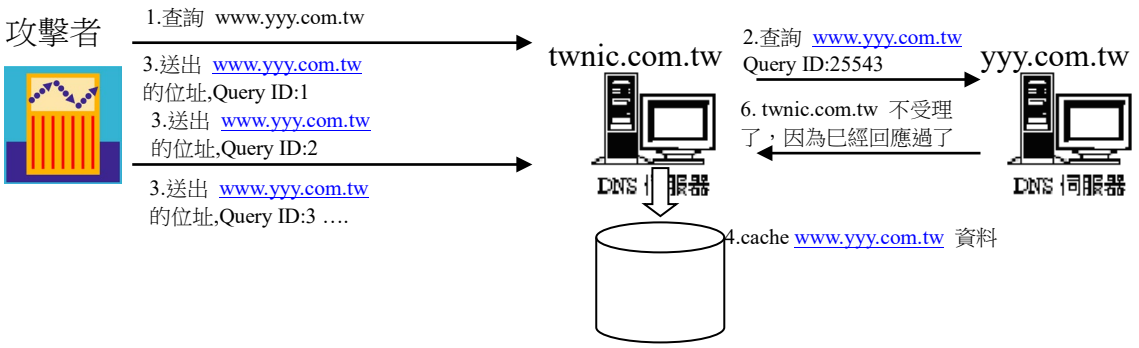
手法二不需以 DNS Server 做為媒介，直接以封包的方式欺騙 DNS



欺騙手法二

手法一二的方法過於簡單，故後來 ISC 即加強此一問題，也就是每原來每個查詢動作皆會保留其 query id 以供識別，不過依據 DNS Packet 特性，Query ID 為 2 bytes，故在數值範圍有限之下(0~65535)，這種問題還是有可能會發生的，尤其是數個版本的 BIND 每次的 Query ID 以加一方式遞增。後來雖改成 Random 方式產生，但系統預設(use-id-pool)並不會保留每次 query 的位址 與 query ID 的對應。所以，若對 DNS 的設定或運作不甚了解的話，問題還是依舊。

即使你使用了 use-id-pool 做 Query ID 的記錄，還是有可能以大量的封包所猜中



我們可以程式產生大量 Query ID 的猜測，甚至連來源位址都設定 yyy.com.tw. ，雖然可能還未猜到 Query ID，正確的 DNS 封包已經回應了，不過做個 N 次總會猜中的，而只要猜中一次對攻擊者而言就已經足夠了，因為他可以將 TTL 值設的相當高。

欺騙手法三

手法四即是以一般的遠程溢位方式，入侵後修改 DNS 資料，將 TTL 值設定最大，然後以程式令外界的 DNS 向其查詢，使用 Cache 此一有問題的資料，即使用日後系統管理人員發現後，要令 DNS 回復正常仍需一段時日，通常這種做法較少人用，但多用於截收 Email 或網站轉向。

任何一種 DNS 欺騙並不限於 A RR，即使反解亦是可以是欺騙的對象，因為反解涉及許多服務的認證，要避免自己成為被欺騙的對像，除了注意版本外，設定要完整，並檢測記錄，或是可以以排程方式定期重啟 DNS 服務亦可。

不安全的 DNS 對企業網路的影響

DNS 失常

這是最常見的情況，使用者會感覺到 DNS 失去作用。此時除了重新啟動，還需去了解為什麼 DNS 會失效。

假造網頁

透過中介 (man in the middle) 的手法，很容易的騙出使用者名和密碼，或者其他敏感資料。其方法如原來您的 Web 主機在 IP1，駭客 DNS 入侵成功後將 Web 指向 IP2，此時使用者以 www.yourdomain.com.tw 來連線時，將指向 IP2，駭客再以映射手法(mirror) 讓使用者覺得網頁是正常的，造成使用者的錯覺。此時即可能騙出使用者登錄時的重要資訊，這種狀況下將損及使用者權益及公司信譽。之前國內曾發生過多起這樣的案例。

複製郵件

所有的信件到達你的服務器之前可以被拷貝，修改或者刪除。入侵者只要了解郵件伺服器與 DNS 的運作原理輕易即可達成此一目的，而其也可以偽造成您的信件寄出，這些都是可以透過 DNS 完成，而您不會感覺到很明顯的異常。其手法同上一段所述。

授權問題

某些與信任有關服務 (如 mail，firewall，proxy 等等) 若涉及 DNS 域名信任時將會無效。如您的防水牆信任 any.com.tw 網域可自由通過，在 DNS 被入侵後防火牆將完全失效。因為入侵者可在您的 DNS 中添加他機器為 any.com.tw 網域機器的資訊。

系統權限

因為部份的 DNS 是以系統管理者權限在運行，當駭客從 DNS 入侵後(指遠端溢位攻擊，remote buffer overflow) ，通常亦直接取得系統權限，即使以非系統權限的身分執行，但依然會有潛在的風險。

資訊洩漏

DNS 設定不正確或不完整，可能造成資訊洩漏的問題，最常見的就是 Zone Transfer。

BIND 9.X 的安全設定：

作者：wuming < mailto:wuming@geekbone.org >
主頁：http://geekbone.org
日期：2001-5-15

我們是否應該注意 DNS 的安全問題？當然，一個管理不善的 DNS 可能帶來以下一些值得一提危險。

1，如果任意允許 zone transfer，一個攻擊者能夠輕而易舉的得到有關 zone 的資訊，這樣其中比如 route，其他重要 hosts/intern hosts 都被泄露。

2，Denial of service，拒絕服務攻擊可能帶來危害：

·你的網站不能訪問，也不能訪問其他網站，因為沒有域名解譯。
·信件不能接收（雖然一些網站有快取，但是不會超過幾個小時或者一兩天時間。）
·攻擊者可以偽裝 DNS 服務提供假的 DNS 資訊。這會帶來什麼后果？

3，徹底沒有防護：如果攻擊者能夠偽造你的 DNS 資料或者欺騙其它網站相信假的 DNS 數據（稱 DNS poisoning），后果不堪設想……

+ 假造你的網頁，並且很容易的騙出使用者名和密碼，或者其他敏感資料。
+ 所有的信件到達你的服務器之前可以被拷貝，修改或者刪除。
+ 如果使用防火墻或者其他服務涉及 DNS 域名相信(auth)的服務，將徹底沒有任何防護作用。比如一個網絡代理只允許 *.mydomain.com 訪問。攻擊者很容易添加他自己的域名。對於防火墻比如只通過 admin.mydomain.com 進入，那麼入侵者添加其 IP 就可以了。

2000 年底由於多個 BIND 遠程溢出，使 DNS 成為黑客最喜好攻擊的目標之一。應該做些什麼？BIND 主要有哪些危險和弱點？

1，首先應該隔離 BIND 服務器，不應該在 DNS 服務器上跑其他服務，尤其是允許普通使用者登入。減少其它的服務可以縮小被攻擊的可能性，比如混合攻擊。

2，雙 DNS 服務器，第二個(secondary DNS)應該安裝在另外一個網絡連接上，(不走同一個 ISP 等)。如果你的 DNS 服務器因為某種原因斷線，至少還有一個快取。這樣一來比如 EMAIL 等都不會丟失。一般可以維持四天(應該能夠修好了吧？！)。

3，使用最新版本的 BIND！（比如 8.2.3 或者 9.1.2）

4，權限管理（Access Control），限制 zone transfer 的範圍，不給攻擊者得到你局域網的資訊。可以使用傳遞簽名(transaction signatures)等。

5，用最低的權限執行 BIND，即非 root 使用者和嚴格的 umask 設置

6，使用 chroot 對執行 BIND 時添加更多的隔離，這樣 BIND 對系統和其他服務帶來修改和破坏會更困難。

7，雖然有些人不相信隱蔽 BIND 的序號對安全有什麼特別的好處，可以有效的組織大多數 script kiddie 的掃瞄。對於專業的駭客是另外一回事。

8，BIND 的紀錄應該常常分析，對於不尋常的記錄可以使用內設的 checker。

9，backend 說：對 BIND（還有其它應用服務）進行安全增強配置的基礎上，安全管理員仍然需要密切關注最新的安全公告、安全補丁和安全技術，經常與專業的電腦安全專家交流知識和經驗。

BIND9 還是 BIND8？
一些值得一提的區別是：

·如果 named.conf 有語法錯誤，BIND9 會記錄錯誤和繼續執行域名服務，而 BIND8 只會記錄錯誤和 segmentation fault 或者 core dump！
·對於事務簽名(TSIG)比 BIND8 有更好的支持。
·新的 start/stop/reload 工具等等。比如 rndc，附有新的 Domain 更新方式。
·zone 文件語法檢測，比如 TTL 行必須存在。
·named.conf 中：
BIND8 中的 check-name 和 statistics-interval 不在使用
缺省屬性 auth-nxdomain 自動為"no"，而 BIND8 是"yes"
·不需要 root 服務器列表，就是 named.boot 或者 root.hint 包含在 server 中了。
·可以使用多進程域名服務（在你的機器 threads 支持良好條件下），如：
% ps ax | grep named
3947 ? S 0:00 /usr/local/sbin/named -u nobody
3948 ? S 0:00 _ /usr/local/sbin/named -u nobody
3949 ? S 0:00 _ /usr/local/sbin/named -u nobody
3950 ? S 0:00 _ /usr/local/sbin/named -u nobody
·BIND9 不支持名字認定，這樣一來你就有可能設置更多的域名，比如下划線。但還是不一定能解釋帶有怪字符域名。
·更多請參閱 http://sysadmin.oreilly.com/news/dnsandbind_0401.html

安裝和設置 BIND
1. cd 至/usr/ports/dns/bind9
2. 執行 make
3. 執行 make install
預設設定檔(named.conf)是在/usr/local/etc 下，執行檔在/usr/local/sbin 中。

設置 chroot：chroot() 設置是為了是 BIND 更加安全，使入侵者即使攻入也無法閱讀任何系統文件，比如多數允許匿名 FTP 使用 chroot()。

假設要設置的目錄在/etc/namedb

1. mkdir /etc/namedb
2. cd /etc/namedb
3. mkdir -p dev etc/namedb var/run
4. cp /etc/localtime etc
5. mknod dev/random c 2 3
6. mknod dev/zero c 2 12
7. 修改/etc/rc.conf 在系統 syslogd 執行參數中加入 –a /etc/namedb/dev/log
8. 起動 named -t /etc/namedb -c /etc/namedb

dig 語法說明：

dig [@server] domain [query-type] [query-class] [+query-option] [-dig-option]

@server: name server
domain: 要查詢的 domain name
query-type: A, MX, NS, SOA...
query-class: in, any
query-option: [no]debug, [no]recurse, [no]vc...

範例：

root@dns ~ > ***dig slhs.tp.edu.tw ns***

```
; <<>> DiG 9.2.2 <<>> slhs.tp.edu.tw ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32981
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;slhs.tp.edu.tw.                        IN      NS

;; ANSWER SECTION:
slhs.tp.edu.tw.         64998   IN      NS      netadm.slhs.tp.edu.tw.
slhs.tp.edu.tw.         64998   IN      NS      dns.slhs.tp.edu.tw.
slhs.tp.edu.tw.         64998   IN      NS      ns2.ntnu.edu.tw.

;; ADDITIONAL SECTION:
dns.slhs.tp.edu.tw.     64998   IN      A       203.72.185.1
netadm.slhs.tp.edu.tw.  64998   IN      A       203.72.185.15

;; Query time: 2 msec
;; SERVER: 163.21.249.166#53(163.21.249.166)
;; WHEN: Fri Nov 21 23:20:36 2003
;; MSG SIZE  rcvd: 126
```

root@dns ~ > ***dig ibm.com ns +norec***

```
; <<>> DiG 9.2.2 <<>> ibm.com ns +norec
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63889
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;ibm.com.                       IN      NS

;; AUTHORITY SECTION:
```

```
com.                    172695  IN      NS      A.GTLD-SERVERS.NET.
com.                    172695  IN      NS      B.GTLD-SERVERS.NET.
com.                    172695  IN      NS      C.GTLD-SERVERS.NET.
com.                    172695  IN      NS      D.GTLD-SERVERS.NET.
com.                    172695  IN      NS      E.GTLD-SERVERS.NET.
com.                    172695  IN      NS      F.GTLD-SERVERS.NET.
com.                    172695  IN      NS      G.GTLD-SERVERS.NET.
com.                    172695  IN      NS      H.GTLD-SERVERS.NET.
com.                    172695  IN      NS      I.GTLD-SERVERS.NET.
com.                    172695  IN      NS      J.GTLD-SERVERS.NET.
```

root@dns ~ > ***dig ibm.com ns***

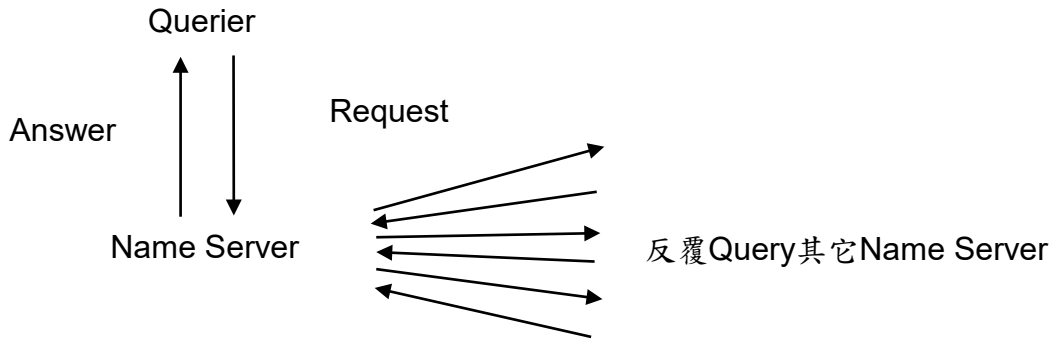
```
; <<>> DiG 9.2.2 <<>> ibm.com ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44136
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ibm.com.                       IN      NS

;; ANSWER SECTION:
ibm.com.                172800  IN      NS      ns.almaden.ibm.com.
ibm.com.                172800  IN      NS      internet-server.zurich.ibm.com.
ibm.com.                172800  IN      NS      ns.ers.ibm.com.
ibm.com.                172800  IN      NS      ns.austin.ibm.com.
ibm.com.                172800  IN      NS      ns.watson.ibm.com.
```

DNS 其它說明：

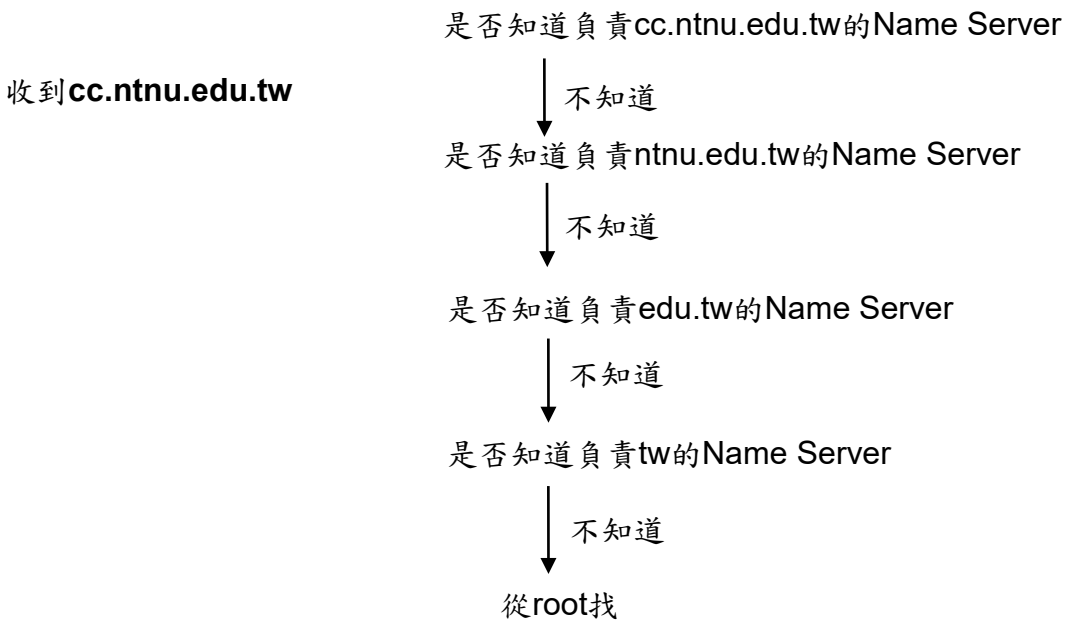
Query Type：
recursive：The name server repeats the same basic process until it receives an answer.



iterative：
-只須回答 the best answer it already known
-告訴 querier 可再查詢的 name server
-對 name server 的負擔較輕

運作原理：
- 當被詢問到有關本域名之內的主機名稱的時候，DNS 伺服器會直接做出回答(此一答案稱為權威回答(Authoritative Answer)，此一主機稱為權威主機)
- 如果所查詢的主機名稱屬於其它域名的話，會檢查快取(Cache)，看看有沒有相關資料
- 如果沒有發現，則會轉向 root 伺服器查詢，然後 root 伺服器會將該域名之授權(authoritative)伺服器(可能會超過一台)的地址告知
- 本地伺服器然後會向其中的一台伺服器查詢，並將這些伺服器名單存到記憶體中，以備將來之需(省卻再向 root 查詢的步驟)
- 遠方伺服器回應查詢
- 將查詢結果回應給客戶，並同時將結果儲存一個備份在自己的快取記憶裡面
- 如果 Cache 資料的時間尚未過期之前再接到相同的查詢，則以存放於快取記憶裡面的資料來做回應

Name server 收到一個 recursive query,本身沒有答案,則會向“closet known” name server 詢問



- 正解 (forward domain): 由機器名稱對應至 IP
  -Forward mapping –Maps all host names to address
- 反解 (reverse domain): 由 IP 對應至網域名稱
  -Reverse mapping –Map address back to host names
  -反解的 DNS Query 遠比正解高出許多，這是一般人常忽略之處
  -Produse output that is easier for human to read
  -Used in some authorization checks
- 正反解一致有其必要
  -國內的系統較不嚴謹，比較不會檢查正反解的一致性，但國外有許多比例都會進行這個部分的確認
  -由來源 IP 查反解名稱，依結果再查正解，並檢驗其結果
  -有部分的 Mail Server 也會使用正反解確認的機制來減少 SPAM 的問題