

DNS 簡介



楊禎葆

abelyang@twnic.net.tw

2002/04/10

內容

- ◆ DNS 早期的發展
- ◆ 什麼是 DNS
- ◆ DNS 的階層式架構
- ◆ 工作原理
- ◆ 與 DNS 相關的服務
- ◆ 相關組織





早期發展

- ◆ Internet 肇發時，尚以 IP 來記憶位址
- ◆ 機器愈來愈多時，使用 hosts 的表格記錄
 - 手工打造
 - 不能學習
 - 不適用大型網路
 - 僅能本機使用
- ◆ 1983 年 P. Mockapetris 建立了第一個 DNS 的規範 (RFC 882)
- ◆ 現今 DNS 已成為 Internet 的基礎建設

DNS 是什麼？

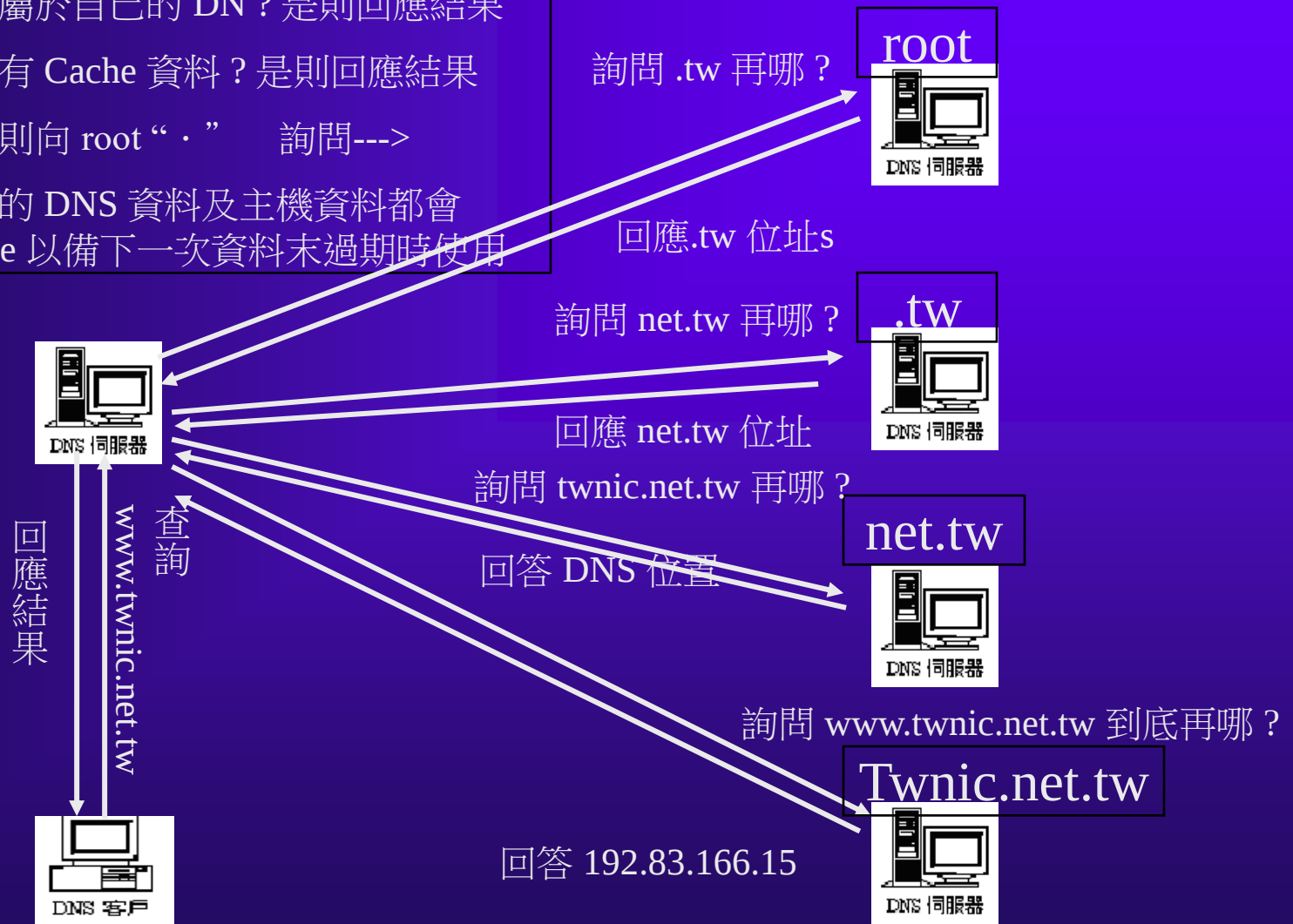
- ◆ 全稱 Domain Name System
- ◆ 用於網路上機器名稱與 IP 的對映關係
- ◆ 以分散式及 Client/Server 的原理來工作
- ◆ 今日的 Internet 上的 Domain Name 已漸成為商標，其即為 DNS 所支持



工作原理

是否屬於自己的 DN ? 是則回應結果
是否有 Cache 資料 ? 是則回應結果
皆非則向 root “.” 詢問---

得到的 DNS 資料及主機資料都會
Cache 以備下一次資料未過期時使用



與 DNS 相關的服務

◆ WWW

- 慣用的 www.DN 結構
- Name-base 的 Virtual Host

◆ Mail

- Mail.DN/DN
- MX Resource Record
- IP Reverse

◆ Security

- 與 IP 認證有關之服務(Firewall, Route...)

◆ 其他

- 諸如 ftp, telnet, login ... 皆與 DNS 相關



相關組織

- ◆ IANA
- ◆ ICANN
- ◆ IETF
- ◆ NIC
- ◆ 其他提供註冊之廠商
 - NSI, VeriSign ...





DNS 介紹及版本分佈

- ◆ 二大類
 - ISC BIND (named)
 - Windows DNS (nt/2000/xp)
- ◆ ISC BIND
 - 共約發行三十幾個版本 (4.X~9.X)
 - 建議使用至少 8.2.3 以上版本
 - 穩定
- ◆ Windows DNS
 - 可見於 Server 級的平台
 - 簡單亦設定是其優點
 - 亦存在漏洞問題



DNS 基本設定

- ◆ ISC BIND (<http://www.isc.org/bind/>) 為介紹基礎
- ◆ 下載及編譯 (請取 8.2.3 以上之版本使用)
 - tar -zxvf bind-8.2.3.tar.gz
 - Make;make install
- ◆ 重要檔案
 - /usr/sbin/named 服務程式(daemon)
 - /usr/bin/nslookup 查詢工具
 - /usr/bin/dig 查詢及多方面的應用工具
- ◆ 所需設定檔
 - /etc/named.conf named 的組態檔
 - /var/named/root.cache Root Server 列表
 - /var/named/ Zone file

named.conf



```
options {                                     // 環境組態 設定
    directory "/var/named";
    allow-transfer { 211.72.210.1/32;};
};
zone "." {                                   // Root Server 的設定
    type hint;
    file "named.ca";
};
zone "abel.com.tw" {                         // 所屬網域名稱
    type master;
    file "/var/named/abel.com.tw.master.hosts";
};
zone "211.72.211.in-addr.arpa" {             // IP 的反解
    type master;
    file "/var/named/211.72.211.rev";
};
zone "aaa.com.tw" {
    type slave;
    masters { 211.72.210.1;211.72.210.10;};
    file "aaa.com.tw.slave.hosts";
}; 以下.... 其他網域名稱或反解...
```

Zone “.”

- ◆ 為 Root Server 表格
- ◆ 可由下列方法取得
 - <ftp://ftp.internic.net/domain/named.ca>
 - `dig @a.root-servers.net > /var/named/named.ca`
- ◆ 共 13 個 Root Server : [a-m].root-servers.net
- ◆ 此表可換成 .tw 的 Root Server 以增效率
 - `dig @a.dns.tw >/var/named/named.ca`

zone “abel.com.tw”



```
$ttl 38400      ; Time to Live , 為 DNS Cache 的時間
@ IN SOA      abel.twnic.net.tw      abelyang.twnic.net.tw. (
    20020410001 ;序號, 用於 Zone Transfer 檢查
    86400        ;更新, 每隔這個時間做 AXFR
    3600         ;重試, 若上失敗則更新改為 3600
    864000       ;過期, 逾時則棄卻此 zone
    38400 )      ;逾時, 3600 x N次 大於此數後即不再 AXFR
    IN NS       ns1      ;即在 TWNIC 指定的名稱
    IN NS       ns2
ns1 IN A       211.72.211.1 ; 同在 TWNIC 指定的 IP
ns1 IN A       211.72.211.2
www  IN CNAME  ns2
abel.com.tw IN MX      10    mail01
abel.com.tw IN MX      20    mail02
mail01 IN A      211.72.211.3
mail01 IN A      211.72.211.4
```

zone “211.72.211.in-addr.arpa”



```
$ttl 38400 ; Time to Live , 為 DNS Cache 的時間
@ IN SOA abel.twnic.net.tw abelyang.twnic.net.tw.(
    20020410001 ;序號, 用於 Zone Transfer 檢查
    86400 ;更新, 每隔這個時間做 AXFR
    3600 ;重試, 若上失敗則更新改為 3600
    864000 ;過期, 逾時則棄卻此 zone
    38400 ) ;逾時, 3600 x N次 大於此數後即不再 AXFR
1 IN PTR ns1.abel.com.tw.
2 IN PTR ns2.abel.com.tw.
3 IN PTR mail01.abel.com.tw.
4 IN PTR mail02.abel.com.tw.
* IN PTR not-use.
```

啟動/停止/除錯

- ◆ 啟動 named
- ◆ 停止 killall named 或 pkill named
- ◆ 除錯 可能的錯誤狀況：
 - 語法錯誤 (reject/syntax error)
 - 不屬於該 Zone (Outside of zone)
 - 沒有 NS 記錄 (no ns RR)
 - 目錄或檔案問題 (No such file or directory)
 - 沒有 Root Server (No root nameservers)
 - 系統問題 (如開啟中的檔案太多, socket port 53 開不啟來)





DNS 安全上的觀念

◆ 防護的觀念

- 僅 Slave 在外服務, 建立 Cache-only 主機
- 至少兩部以上的 DNS (容錯/負載平衡/系統安全)
- 限制 AXFR 範圍
- 主機上僅開啟必要的服務
- 使用 BIND 時, 版本至少 8.2.3 以上
- 注意 dns 所產的 log

◆ 遭人入侵後可能的結果

- 以中介的手法 (man in the middle) 騙取資訊
- 攔截郵件
- 信認問題
- 取得系統權限並濫用



BIND 9 特點與BIND 8 之比較

- ◆ 兩者之差異
- ◆ BIND 9 的新功能
 - 工具
 - 語法檢查的工具
 - DNSSEC Key 的產生工具（另有介紹）
 - 設定項目
 - IPv6 相關功能
 - DNSSEC 相關功能
 - 反解項目
 - 設定檔（ `named.conf` ）中新的項目
- ◆ 如何取捨使用 BIND 8 或 BIND 9

兩者差異

版本	8.X	9.X
編譯	傳統的 Makefile	較人性的 autoconf
工具程式	查詢，診斷，動態更新，轄區傳送	DNSSEC，語法檢查，診斷，動態更新，(預計捨棄 nslookup 而用 dig)
執行狀況	單一執行程式	多緒(mutli-thread) 多 CPU 的支援
除錯	僅能從記錄檔分析	提供工具做語法檢查
IPv6	簡單的支援 (AAAA)	多了 A6 offset 的功能
反解	只有一種方法	共三種方法且簡單，對 IPv6 的特性更容易處理
資料庫	無	宣稱可支援多種不同的資料庫
資料格式	僅 7bit 資料	可使用 8bit 資料



BIND 9.X 新功能——新的工具

- ◆ `named-checkconf [filename]`
 - 做 `named.conf` 的檢查
- ◆ `named-checkzone [-c class] zone [filename]`
 - 做 zone file 的的 check



BIND 9.X IPv6(1) 設定部份

- ◆ `listen-on-v6`
- ◆ `transfer-source-v6`
- ◆ `notify-source-v6`
- ◆ `query-source-v6 address *`
`port *`

BIND 9.X IPv6 (2) 表示法

- ◆ `XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX`
- ◆ 128 bits 固定長度,每16 bits 以 : 隔開, 共 8 個欄位
- ◆ 每一欄位開頭的 0 可省略
 - Ex: 2001:238:882:0:248:54ff:fe53:d3ee
- ◆ :: 可代表連續多個 0 的欄位(僅可使用一次)
 - 2001:238:F882:0:0:0:0:1 = 2001:238:F882::1
 - 0:0:0:0:0:0:0:1 = ::1
 - 0:0:0:0:0:0:0:0 = ::
 - 2001:0:0:345:0:0:0:1 = 2001:0:0:345::1
- ◆ 16 個 bytes 誰記得住呢 ?

BIND 9.X IPv6 (2) 資源記錄

- ◆ 除了原有的 AAAA 外,新加了 A6 Chain 的概念
\$ORIGIN example.com.

```
host 3600 IN A6 64 0:0:0:0:42::1  
company.example1.net.
```

```
host 3600 IN A6 64 0:0:0:0:42::1  
company.example2.net.
```

```
$ORIGIN example1.net.
```

```
company 3600 IN A6 0  
3ffe:8050:201:1860::
```

```
$ORIGIN example2.net.
```

```
company 3600 IN A6 0  
1234:5678:90ab:fffa::
```

BIND 9.X 反解 (1)

◆ 原有的反解格式 (Nibble Format)

\$ORIGIN 3. 2. 1. in-addr. arpa.

4 86400 IN PTR host4. twnic. net. tw.

◆ 位元直接轉換 (Bitstring Format)

\$ORIGIN \[x3ffe805002011860/64]. ip6. arpa.

\[x0042000000000001/64] 14400 IN PTR host4. twnic. net. tw.

\$ORIGIN \[1. 2. 3/24]. in-addr. arpa.

\[4/24] 14400 IN PTR host4. twnic. net. tw

BIND 9.X

反解 (2)

◆ 使用 DNAME (可用於正解部份)

在兩段反解中的格式如下

(1) \$ORIGIN \[x00aa00bbcccc/48]. ip6. arpa.

\[xdddd/16] IN DNAME ipv6-rev.example.com.

(2) \$ORIGIN \[x666655550004/48]. ip6. arpa.

\[x0001/16] IN DNAME ipv6-rev.example.com.

在 zone ipv6-rev.example.com 上再做實際反解

\$ORIGIN ipv6-rev.example.com.

\[x1234567812125675/64] IN PTR host.example.com.

BIND 9.X

反解 (3)

◆ \$GENERATE 變數迴圈 (可用於正解部份)

;用於反解

```
$ORIGIN 3.2.1.in-addr.arpa.
```

```
$GENERATE 0-255 $ PTR host$.tw.nic.net.tw.
```

;用於正解

```
$ORIGIN tw.nic.net.tw.
```

```
$GENERATE 0-255/10 $host A 1.2.3.$
```



設定檔 (named.conf → View

- ◆ View 針對不同的 IP 有不同的限制

語法:

```
view "view_name" {  
    match-clients { address_match_list };  
    [ view_option; ... ]  
    [ zone_statement; ... ]  
};
```

範例:

```
view "view_name1" {  
    match-clients { 10.0.0.0/8; };  
    recursion yes;  
    zone "example.com" {  
        type master;  
        file "example-internal.db";};  
};  
};
```



設定檔 (named.conf)—rrset-rrorder

- ◆ rrset-order 多筆 FQDN 時回應的方法

語法：

```
rrset-order {      [ class class_name ]  
                  [ type  type_name ]  
                  [ name "domain_name";]  
                  order ordering;  
                }; // ordering:fixed/random/cyclic
```

範例：

```
rrset-order {class    IN type A name "twnic.net.tw";  
              order random;order cyclic;};  
rrset-order { class    ANY      type ANY      name "*";  
              order cyclic ;};
```

如何取捨 8.X 或 9.X

- ◆ 預設安裝之問題
- ◆ 視需求而定
 - IP 數量是否眾多
 - 網路是否常變動
 - 是否使用 IPv6
 - 是否使用中文域名
 - DNS 查詢量是否龐大
 - 對安全的要求等級
 - 公司性質而定

