竹苗區網
DNS教育訓練

國立交通大學 資訊技術服務中心
蘇俊憲
2015.11

Outline

1.DNS基礎概念

2.DNS放大攻擊介紹

- 2.1防治方法

3.DNS架設

- 3.1 Resolver (Cache Only)
- 3.2 Authoritative(權威伺服器)

DNS 管理 – 基礎篇

DNS基礎概念

網域名稱(Domain Name)是什麼?

- 網域名稱是企業或個人在網路上的身份，
  - 如同 IP Address 一樣，都具有唯一的特性
  - 網域名稱比 IP 好記
  - 好記的網域名稱成為大家申請的對象
    - 字數少/特殊意義單字/諧音字

備註:

- 網域名稱(台灣) vs. 域名(大陸)

DNS 背景介紹

- Domain Name System(DNS)的歷史
  - IP Network 的興起,網網互連
  - 愈來愈多的主機, hosts 檔的出現
    - 主機名稱的衝突
    - 資訊的一致性
    - 資料的管理
- 1984年Paul Mockapetris 建立了第一個DNS 的規範(RFC1034， RFC1035)
  - 1985 年隨即出現了第一個網域名稱

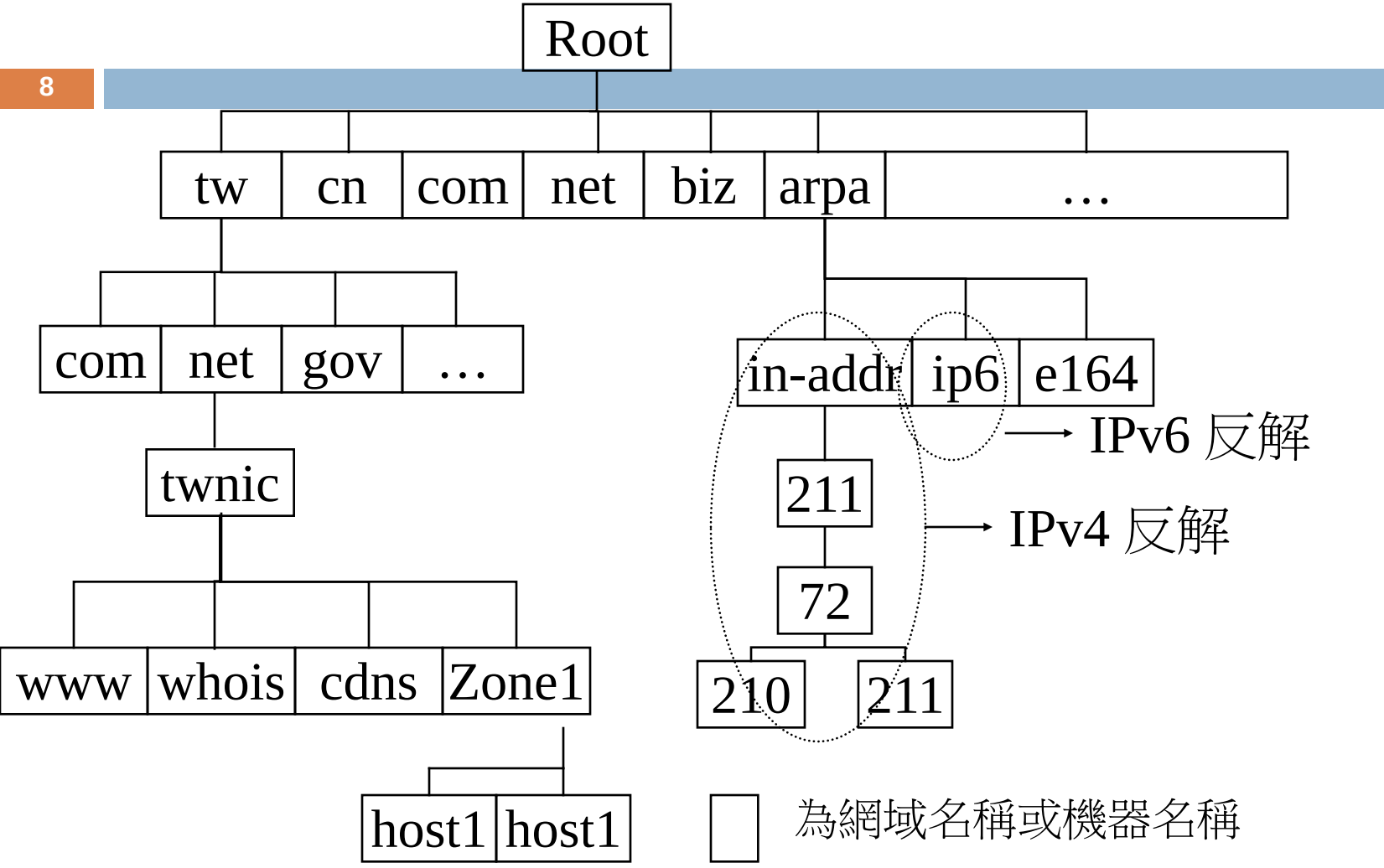
網域名稱與Internet相關服務之關係

- 名稱解析服務為 Internet 服務最基礎的一環
  - TWNIC 被列為國內20最重要的資安單位
- 名稱解析提供機器名稱與 IP 位址雙向對映的機制
  - WWW: www.hinet.net <-> 168.95.1.82
  - MAIL: msa.hinet.net <-> 168.95.4.211
- 網域名稱比 IP 容易記， 且具代表意義
- 使用網域名稱讓系統更具移值性，當 IP 變動，只需更改 DNS 設定即可，程式 網頁等不需更改

DNS查詢服務--運作模式

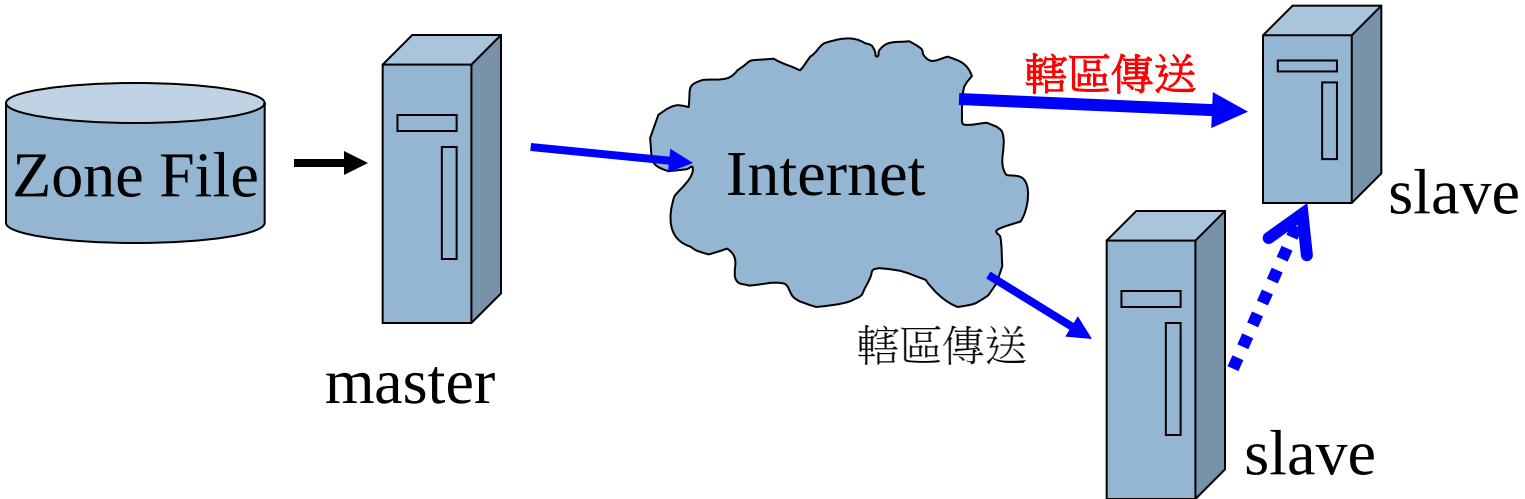
- 分散式 - 全球最大的分散式資料庫系統
  - 自家domain zone資料由自己(或授權單位)維護，而其他 domain zone的資料則分散在全球眾多的 DNS servers 上
  - Domain zone資料同步: 可由 Master 主機自由複製到 Slave 主機
- On Demand & Tree Structure
  - 沒有一台DNS伺服器會有全部的DNS資料
  - 以樹狀結構的方式找到目的位址(每個結點需要授權)
    - 經由全球統一的 Root Server Group 達到正確搜尋的目的
  - Root Server 表面上共十三部，但實際每一部可能都有許多 Mirror (如 f.root-servers.net 有二三十部)
    - http://www.root-servers.org/ 目前 Root Server 分布情形
- 穩定 - 負載分散 (load sharing) 與備援
  - 一個網域名稱可由多台主機共同服務(流查詢)
- 效率
  - 主要使用UDP 封包, 查詢速度基本上都在 100 msec 內
  - 經由 Cache 來加快 DNS 的查詢

DNS zone – 樹狀結構



DNS伺服器 - 簡單分類（1/2）

- 權威主機(Authoritative)- 針對特定 domain zone, 可管理或回答其網域名稱之答案
  - Master server 所管轄的資料是從本機的硬碟檔案（Zone File）中而來
  - Slave server 的資料是以轄區傳送(Zone Transfer) 從其他 authoritative Server（master or slave）而來
  - 參考指標
    - 指標1: Zone file 的 Data Entry, 其 TTL 不會改變
    - 指標 2: 是否登記註冊（e.g., hidden authoritative servers）



DNS伺服器 – 簡單分類（2/2）

- Resolver（Cache-Only）主機
  - 即沒有管理自家任何的網域名稱，僅接受DNS查詢與回應，並將其快取以方便往後使用
  - 參考指標
    - 所留存的 DNS Entry，TTL 會隨時間遞減（減到0，該筆資料就失效）

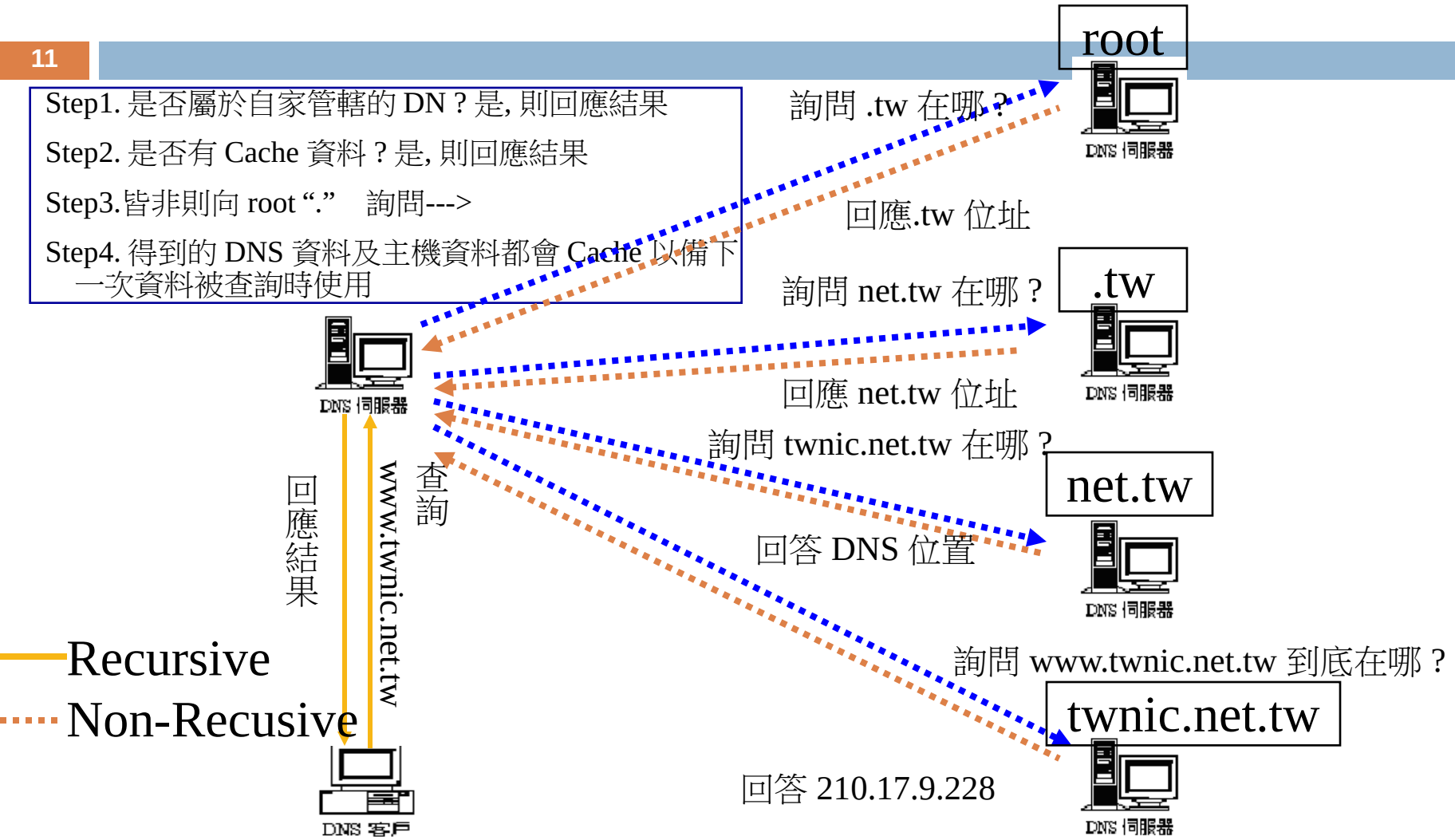
DNS 查詢運作原理 圖示

Step1. 是否屬於自家管轄的 DN？是, 則回應結果

Step2. 是否有 Cache 資料？是, 則回應結果

Step3. 皆非則向 root "." 詢問--->

Step4. 得到的 DNS 資料及主機資料都會 Cache 以備下一次資料被查詢時使用



DNS查詢 – 運作原理補充(1)

- 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

DNS查詢 – 運作原理補充(2)

- 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

常見的DNS server平台

- ISC BIND
  - 目前最常見的DNS servers 軟體
  - 建議使用 BINDv9 的穩定版
    - 發行超過五十個版本 (4.X~9.X)
    - 最新版本資訊,參見ISC首頁(http://www.isc.org)
  - 多建置於UNIX platform (但也有轉殖到Windows 的版本)
- Windows DNS Server
  - 可見於 Windows Server 級的版本
  - 根據 BIND 4.x 修改而來,並持續更新
  - GUI 設定 - 簡單設定是其優點

正解/反解之意義與原理

- 正解 (forward domain): 由機器名稱對應至 IP
- 反解 (reverse domain): 由 IP 對應至網域名稱
  - 正解的 DNS Query 遠比反解 (主要 PTR)高出許多
  - 向 ISP 提出 IP 建立反解的需求
- 正反解一致有其必要性
  - 雖然多數的系統不強求正反解一致性,但少數的公司或學校對此仍有要求
  - 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

DNS 相關議題

- 用 BIND 還是用 Windows DNS ?
- 設定檔 named.conf
  - 根伺服器介紹與設定
- zone file基本設定
  - 資源紀錄（SOA，NS，A，CNAME，MX，PTR…）
  - 正解/反解設定
- 主要（master）/附屬（slave）伺服器的關係
  - 容錯及負載平衡功能（Round Robin）
- named之參數說明及啟動與停止
- BIND 工具程式
  - named-checkconf
  - 使用 nslookup/dig 自我檢測

用 BIND 還是用 Windows DNS ?

	Windows	BIND
操作	●GUI的設定方式入門容易 ●可用 Windows 其他服務結合 (WINS/AD)	●設定以文字編輯進行 ●入門時,文字工作較易出錯 ●Unix 環境為一般人所不熟悉
效率	●查詢數字無非官方統計資料	●每秒可處理上萬次查詢 ●Multi-thread/SSL
穩定性	●視 OS 表現 ●基本上可符合一般企業需求	●穩定性佳 ●版本更新速度較快
安全性	●隨系統版本更新而更新版本	●可從設定面加強安全性 ●較能預防DNS Spoofing
佔有率	●在台灣兩者相當	●在全世界佔大宗
其他		●Root Server 皆以 BIND 為主

設定檔: named.conf

- BIND（named）環境之主要設定檔
  - 路徑 - /etc/named/named.conf 或 /usr/local/etc/named.conf
- 作用 - 定義特定 DNS server 所提供的服務
  - 定義 named 的功能項目 （ options ）
  - 定義 root server 位置 （ zone ）
  - 定義所管轄之網域名稱 （ zone ）
  - 定義反解 （ zone ）
  - 其他，如系統記錄/存取控制列表等…

named.conf: options


```
#/etc/named/named.conf
options {
directory "/var/named";
pid-file “/var/named/named.pid”;
allow-transfer     { 211.72.211.71/32;211.72.210/24;};
};
```

Directory	zone file 檔案存放位置（預設為 /etc）
pid-file	DNS 啟動時記錄行程代號(PID)之檔案
allow-transfer	轄區傳送之設定，定義那些 IP 可與此部 DNS 做 AXFR（未定義則全開，形同 DNS 資料外流）

- 常犯錯誤
  - options 忘了加 “s”，前後以 {} 括住
  - 有關檔案或路徑名稱皆要加 “” 號
  - 每一個描述（statement）的結尾需有 “;” 號
  - 有關 IP 等設定項目亦需加 ; 號
  - pid-file 所指路徑的權限問題要注意

在named.conf設定根伺服器


```
zone “.” {
        type hint;
        file “root.cache”;
};
```

- 所有的 DNS 伺服器皆需要知道根伺服器位置
- 根伺服器為所有 DNS 查詢之起源
- hint 字面為暗示之意，即向 DNS 表示如果你沒有資料，可以到根伺服器詢問
  - 一部 DNS 僅能有一 hint type
- 根伺服器列表可由 ftp://ftp.internic.net/domain/named.cache 取得

在named.conf設定正解網域


```
zone   "xxx.edu.tw"   {
        type master;
        file "Z-xxx.edu.tw";
        allow-transfer { 168.95.1.1;168.95.192.1;};
        }; /* 上述 Domain zone name 和 IP 僅為範例 */
```

- 此一域名需上層授權(edu.tw) 後別人方可查得到
- 若您有多個網域名稱即添加類似設定即可
- 此例為 master 主機設定，slave 主機設定於後述
- file **相對路徑**即表參照 directory 參數
- 注意 ; 號問題
- 此處的 allow-transfer設定 僅對此網域 (zone, xxx.edu.tw)有效，而options 中的 allow-transfer 則對此部 server 所管轄的全部 DNS zones 都有效

在named.conf設定反解網域


```
zone  "0.0.127.in-addr.apra"  {
      type master; file  "named.local";
};
zone  "210.72.211.in-addr.arpa"  {
      type master;
      file  "R-211.72.210";
};
```

- in-addr 為 Internet Address 之意，用於 IPv4 之反解，IPv6 則使用 ip6
- apra 為美國國防部計畫的縮寫
  - 目前 Internet 為早期 Arpa 計畫之一
  - 反解起源之 TLD,其他諸如與”數字”有關之解析多以 arpa 為 TLD

named.conf 完整內容範例


```
#/etc/named.conf
options {
     directory "/var/named";
     pid-file  “/var/named/named.pid” ;
# only for slave or none, default is any
    allow-transfer    { 211.72.211.71/32;211.72.210/24;};
};
zone  “.”  {
    type hint;
    file  “named.cache” ;
};
zone  “xxx.com.tw”  {
    type master;
    file  “xxx.com.tw.hosts” ;
    allow-transfer { 168.95.1.1;168.95.192.1;};
    };
zone  “0.0.127.in-addr，apra”  {
    type master;
    file  “named.local” ;
};
zone  “210.72.211.in-addr.arpa”  {
    type master;
    file  “211.72.210.rev” ;
};
```

named.conf 回顧

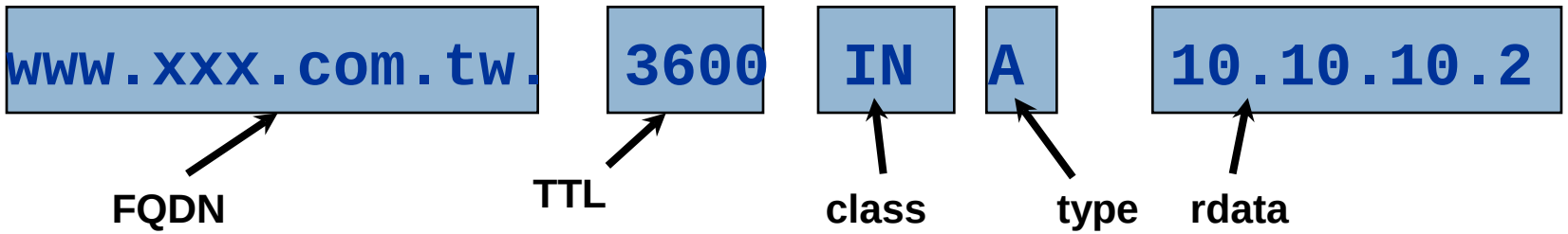
- 基本設定
  - options
  - root_server
  - 正解/反解 domain zones
- 常犯錯誤
  - 語法及 ; {} “” 等問題需注意（初學常犯）
  - 檢查工具: 可使用工具程式 named-checkconf，named-checkzone 幫您做語法檢查
- 注意 Zone Transfer 問題
- 若欲為 Cache-Only 主機則可拿掉 正解/反解設定即可（即保留 options/root/localhost）

DNS 基礎篇 – Zone File

Zone File 的設定

正解: 什麼是資源記錄

- 資源記錄(RR， Resource Record)
  - 名稱(FQDN) → **所要(等待)查詢的問題**
  - 快取時間 (TTL，Time to Live)
  - 網路類別(class)，
  - 資料類型(type)
  - 答案(rdata)
- TTL 是此一筆資料被別的 DNS Cache 的時間值
- IN 即是 Internet
- 資料類型分許多種
- 下列為一筆資源紀錄的內容

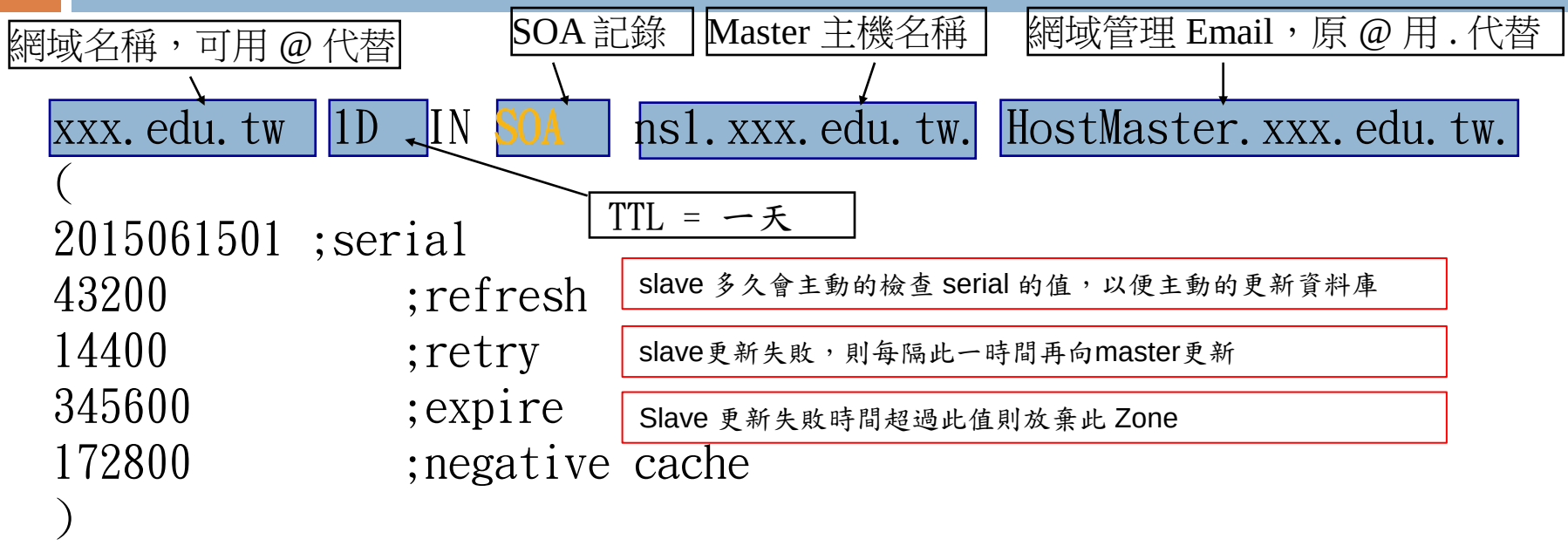


範例: 正解資源記錄


```
$TTL  1D;  /* 新版, Default TTL = 86400 seconds */
@  38400 IN SOA FalseDNS.xxx.edu.tw.  HostMaster.xxx.edu.tw. (
     2010073101      ; Serial
     43200           ; Refresh 12 hours
     14400           ; Retry 4 hours
     345600          ; Expire 4 days
     7200            ; Negative cache 2 hours
     )
xxx.edu.tw.          86400    IN    NS     ns1.xxx.edu.tw.
xxx.edu.tw.          86400    IN    NS     ns2.xxx.edu.tw.
ns1.xxx.edu.tw.      86400    IN    A     211.72.211.1
ns2.xxx.edu.tw.      86400    IN    A     211.72.211.2
 ; 以下略
```

- 資源記錄的 TYPE 有許多不同類型

典型的 SOA RR



- SOA（Start Of Authority）記錄用於DNS自身,代表其為權威主機
- SOA 提供此一 Zone 之基本資料及更新時間參數供 Slave DNS 更新使用

NS/A RR


```
xxx.edu.tw.    IN   NS   ns1.xxx.edu.tw.
xxx.edu.tw.    IN   NS   ns2.xxx.edu.tw.
ns1.xxx.edu.tw.   IN   A   211.72.211.1
ns2.xxx.edu.tw.   IN   A   211.72.211.2
```

- 每個 Zone File ，如同 SOA 一般，皆必須要有 NS RR 。
  - NS 記錄說明了那些主機管理此一網域名稱（權威主機），需與上層（如教育部, 區縣網, 各級學校）的指定一致
- NS 記錄之 RDATA 需接一 FQDN 記錄，不可用 IP ，也不可接到一 CNAME 記錄（ RFC 規範）
- 接於 SOA 之後NS RR 之 RDATA 若屬同一個zone以內者(如上例)，則比須接著定義對應的 A (Address) RR (i.e., Glued Records) ，以標明其 IP Address
  - NS 記錄對應的 A RR 所指之 IP 不能是 Private/Loopbak/multi-cast 等 IP
- NS 記錄的取用順序是隨機決定的，而非取用第一筆

兩部以上 DNS 之作用

- 根據 InterNIC 的規定，NIC 之 DNS 指定應兩部以上
- 兩部 NS 之意義在於
  - 容錯:只有一部 DNS 失效時，眾多網路服務也跟著失效，且正確的兩部以上主機更應處在不同的網段以降低風險
  - 系統安全 : 二部以上的 DNS 主機能互相支援，亦爭取了足夠的處理時間，也有效的降低網路安全的風險
  - 負載分攤

    若您設定了兩部以上的 DNS 主機，當有人連接您的網站前，其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

Master/Slave 如何實現

ns1.xxx.edu.tw

```
#/etc/named.conf
#其他略
zone "xxx.edu.tw" {
        type master;
        file "xxx.edu.tw.hosts";
        allow-transfer {
            211.72.211.2/32;
        };
};
```

ns2.xxx.edu.tw

```
#/etc/named.conf
#其他略
zone "xxx.edu.tw" {
    type slave;
    masters {211.72.211.1;};
    file "Z-xxx.edu.tw";
    allow-transfer {none;};
};
```

- 一般而言 Slave 主機應不允許 zone transfer
- Slave 主機啟動後即會和 Master 同步資料，而後資料的同步即是參考 SOA 資訊
- Master 主機更改了資料請務必記得序號需加大，否則即使時間到了 Slave 不會同步資料

Master/Slave 的同步問題

- Zone transfer 只有一個方向，由 Slave 向其他 authoritative Server (Master or 另一 slave) 發出要求
- 如果 Master 更改了資料，以上述 Zone File 的範例而言，最長要一天後 Slave 才會更新，顯然不夠即時

- 解決方法
  - 降低 Refresh 之值：或可改善但仍會有時間差
  - 使用 Bind 8.x/9.x 之 notify 功能
    - 當 Master 重新啟動時，即會送出 notify 訊息至所有 Zone File 中的 NS RR，告知這些機器進行 AXFR
    - 這個功能在 Bind 9.x 中預設即已啟動，若欲關閉

```
options { ….
    notify    no;
};
```

子網域的分割(授權管理)


```
;在 xxx.edu.tw. 的 Zone File 內
$ORIGIN xxx.edu.tw.
             IN    NS    ns1
             IN    NS    ns2
ns1          IN    A     211.72.211.1
ns2          IN    A     211.72.211.2
;ws1.dept1.xxx.edu.tw.     IN     A      211.72.211.101

$ORIGIN    dept1.xxx.edu.tw.
             IN    NS    ns1
             IN    NS    ns2
ns1          IN    A     211.72.211.101
ns2          IN    A     211.72.211.102
```

- 上述例子 dept1 部門, 需要自建一 Sub-domain，以管理自己部門之 DNS 資料，則上層需定義對應NS 記錄再授權出去
- 於 ns1.dept1.xxx.edu.tw 及 ns2 上再建立 dept1.xxx.edu.tw. 的 Zone File，並做好 Master/Slave 之區分
  - 如果原在上層 Zone File 中有定義相關資料（如 ws1.dept1.xxx.edu.tw）應從 xxx.edu.tw. 中移除（已授權子網域 dept1.xxx.edu.tw 管理）

CNAME（Canonical Name）RR

www.xxx.edu.tw. 3600 IN A 211.72.211.80
ftp.xxx.edu.tw. 3600 IN CNAME www.xxx.edu.tw.

- CNAME 用於機器別名，如查詢 FTP ，則會查到 WWW 位址
- 建議使用 A 記錄來替 CNAME，以避免 NS/MX 等出現問題
- CNAME Chain 問題，雖沒有禁止使用，但會導致效率變差甚至錯誤

MX（Mail eXchange）RR


```
@       IN   MX   10   mail
@       IN   MX   20   imap
mail    IN   A        211.72.211.25
imap    IN   A        211.72.211.143
;此時不可用如 mail IN CNAME www 語法
```

- MX（Mail eXchange）記錄為 SMTP 服務所使用，其中的 10，20 表示郵件交換時的優先順序(數字小者優先)
- 亦可使用 A 記錄 (hidden MX RR)來代表 MX使用（即 DN=FQDN)，但如此僅能使用一部機器當 Mail Server
  - *如上例,* @ IN A *211.72.211.25*
- 相關課題:
  - Hotmail/Yahoo/Google 的 MX 有什麼玄機 ?

正解檔完整內容範例


```
xxx.com.tw.      86400 IN SOA    ns1.xxx.com.tw.
root.xxx.com.tw. (
    2002021301     ; serial
    1D         ; refresh
    1H         ; retry
    1W         ; expiry
    2D          ; negative cache
)
xxx.com.tw.          86400    IN    NS    ns1.xxx.com.tw.
xxx.com.tw.          86400    IN    NS    ns2.xxx.com.tw.
Ns1.xxx.com.tw.      86400    IN    A     211.72.211.1
Ns2.xxx.com.tw.      86400    IN    A     211.72.211.2
www.xxx.com.tw.      86400    IN    A     211.72.211.80
ftp.xxx.com.tw.      86400    IN    CNAME     www.xxx.com.tw.
xxx.com.tw.     86400    IN     MX     10     mail.xxx.com.tw.
xxx.com.tw.     86400    IN     MX     20     imap.xxx.com.tw.
mail.xxx.com.tw.     86400     IN     A     211.72.211.25
imap.xxx.com.tw.     86400     IN     A     211.72.211.143
wk1.dept1.xxx.com.tw.     86400     IN     A     211.72.211.101
wk2.dept1.xxx.com.tw.     86400     IN     A     211.72.211.102
```

- 從上述來看是不是又臭又長呢 ？

以 $TTL/$ORIGIN 來簡化設定


```
$TTL    86400          ; 預設 TTL 值，原來每筆 RR 之 TTL 值可以此值代替
$ORIGIN    xxx.com.tw.   ; 預設附加字尾如同該 zone 則可不寫

@          IN     SOA    ns1     root (
    2002021301     ; serial
    1D         ; refresh
    1H         ; retry
    1W         ; expiry
    2D          ; negative cache
)
             IN    NS    ns1
             IN    NS    ns2
             IN    MX    10    mail
             IN    MX    20    imap
ns1          IN    A     211.72.211.1
ns2          IN    A     211.72.211.2
www          IN    A     211.72.211.80
ftp          IN    CNAME     www
mail         IN    A     211.72.211.25
imap         IN    A     211.72.211.143

$ORIGIN dept1.xxx.com.tw.
ws1          38400     IN    A     211.72.211.111
ws2          38400     IN    A     211.72.211.112
```

反解域名設定 （named.conf）


```
Zone "210.72.211.in-addr.arpa" {
    type master;
    file "210.72.211.rev";
};
```

- 反解依然有 master/slave 主機之分，與正解同理
- 上例為一 Class C 反解，若為 Class B 則可寫成 72.211.in-addr.arpa.
- 若不滿一個 Class C，設定方法較特別，請參考網址 http://dns-learning.twnic.net.tw/DNS94/

範例：反解Zone File內容


```
$TTL 86400
$ORIGIN     211.72.211.in-addr.apra.
      IN      SOA      ns1.xxx.com.tw.      Root.xxx.com.tw. (
      20030421;
      86400;
      3600;
      864000;
      2D;
)
      IN      NS       ns1.xxx.com.tw.
      IN      NS       ns2.xxx.com.tw.
1      IN      PTR      ns1.xxx.com.tw.
2      IN      PTR      ns2.xxx.com.tw.
3      IN      PTR      pc3.xxx.com.tw.
; 以下類推…..
```

- 反解之 Zone File 內容與正解類似
- 反解之 TYPE 為 PTR (Pointer)，指出這個 IP 對應什麼名稱
- 建議正反解最好一致

反解: 利用 $GENERATE 變數簡化


```
;前 SOA 及 NS RR 略
1       IN          PTR     pc1.xxx.com.tw.
2       IN          PTR     pc2.xxx.com.tw.
3       IN          PTR     pc3.xxx.com.tw.
...
31      IN          PTR     pc31.xxx.com.tw.
```

- 上述例子可以 BIND 9.X 之 $GENERATE 功能表示為:

```
$GENERATE 1-31     $     PTR     pc$.xxx.com.tw.
; $ 即表 1-31，將會自動展開成 31 行的 PTR
; BIND 9.X 省略 IN (Class) 不寫
```

- $GENERATE 亦可用於正解部分，語法相同

負載分攤功能（Round Robin）


```
www     IN    A    211.72.211.80
www     IN    A    211.72.211.81
pc1     IN    A    211.72.211.80
pc2     IN    A    211.72.211.81
```

- DNS 僅做名稱之負載分攤（load sharing）
  - 祥見 本課程 DNS 管理進階編（後半）
  - 如 www/mail 或他類型的服務之負載平衡（load balance）要取決其他技術(e.g., Level 4 switch)
- 如上資料，一個 FQDN 可有兩個以上之 IP 位址
- DNS server 所回應的答案基本上是循環的（round-robin）
  - 在 BIND 9.X 中可以改變這個順序（依據/etc/named.conf系統設定 rrset），不過一般是較少用到

DNS Running ?

- 如何確定 DNS 是否運行呢 ?
  - Port Scan 目標 53/UDP (敏感動作)
  - nslookup -q=ns . Dns_server (查詢其 Root 記錄)
  - dig @dns_server . Ns
- DNS 不正常原因:
  - 語法錯誤造成 DNS 未啟動
  - 觀念錯誤造成運作不正常
  - 版本差異與認知上之問題 (BINDv9 vs. BINDv8)
  - 網路是否正常 (流量，斷線…)
  - 是否被 Router/Firewall 等檔掉了 53 port
  - 被入侵或欺騙
  - 判別密碼被猜出或離職員工惡意或其他非故意而被人為的改變了 DNS 的指向
  - 是不是 TWNIC 的關係造成解析上的問題
  - 其他

檢測工具: nslookup/dig

- nslookup
  - UNIX 及 Windows 平台皆有
  - 可使用命令模式與交談模式
  - 較好用但資訊較簡略
- dig
  - 僅有命令模式
  - 較不好用但資訊完整

以nslookup追蹤(1)


```
[root@pc071 named]# nslookup
Default Server:  ns1.xxx.com.tw
Address:  211.72.211.1

> set q=soa
> xxx.com.tw.
Server:  pc071.twnic.net.tw
Address:  211.72.211.71

xxx.com.tw
        origin = ns1.xxx.com.tw
        mail addr = root.xxx.com.tw
        serial = 2002021301
        refresh = 86400 (1D)
        retry   = 3600 (1H)
        expire  = 604800 (1W)
        minimum ttl = 172800 (2D)
```

啟動 nslookup 交談模式
連線至 nameserver

設定查詢類別為 SOA 資訊
查 xxx.com.tw.

如 Zone 所列之內容(SOA 訊息)

以nslookup追蹤(2)


```
;續前頁
xxx.com.tw          nameserver = ns1.xxx.com.tw
xxx.com.tw          nameserver = ns2.xxx.com.tw
ns1.xxx.com.tw      internet address = 211.72.211.1
ns2.xxx.com.tw      internet address = 211.72.211.2
```

- set q=soa 之功能，除 SOA 外，您尚可設定其他 TYPE（如 NS，A，MX，CNAME，PTR ...等不同記錄），以查到您想要的資訊
- 命令模式（等同與上例）

  nslookup -q=soa xxx.com.tw.

以nslookup追蹤(3)


```
[root@pc071 named]# nslookup
Default Server:  ns1.xxx.com.tw
Address:  211.72.211.1

> server dns.hinet.net
Default Server:  dns.hinet.net
Address:  168.95.1.1
> set q=ns
> hinet.net
Server:  dns.hinet.net
Address:  168.95.1.1
;以下結果略

>ls -d hinet.net
[dns.hinet.net]
*** Can't list domain hinet.net.: Unspecified error

>server ns1.xxx.com.tw.
>ls -d xxx.com.tw.
;以下會列出 xxx.com.tw. 的 Zone File 內容
```

以 dns.hinet.net 做為 DNS Server

設定查詢 NS 記錄

對 dns.hinet.net 要求 ls (list) -d(domain) 資料 (即 AXFR)，結果當然被拒ls -d 之指令不適用於 BIND 9環境

(省略部份訊息)，切回 ns1 並做 AXFR，若允許 Client IP 做 AXFR 則會列出 Zone File 內容

以nslookup追蹤(4)


```
>set q=a
>www.xxx.com.tw.
Server:  ns1.xxx.com.tw
Address:  211.72.211.1

Name:    www.xxx.com.tw
Addresses:  211.72.211.80，
          211.72.211.81

>www.msn.com.
Server:  ns1.xxx.com.tw
Address:  211.72.211.1

Non-authoritative answer:
Name:    www.msn.com
Addresses:  207.68.171.245，
          207.68.171.247， 207.68.172.234，
          207.68.173.244， 207.68.173.254，
          207.68.171.244
```

查詢 www.xxx.com.tw.資訊，列出兩個 IP，即是此記錄做 Round Robin，再查一次可能是相同順序，亦可能 81 會排到前面，如果您在看此網站，有時可能會連到 80，但有時又會連到 81，即可達到負載平衡之效果

查詢外面的網域名稱可以查的到，代表root server的設定正常

Non-authoritative answer 表示為非權威資料，意即是 Cache 而來

以dig追蹤(1)

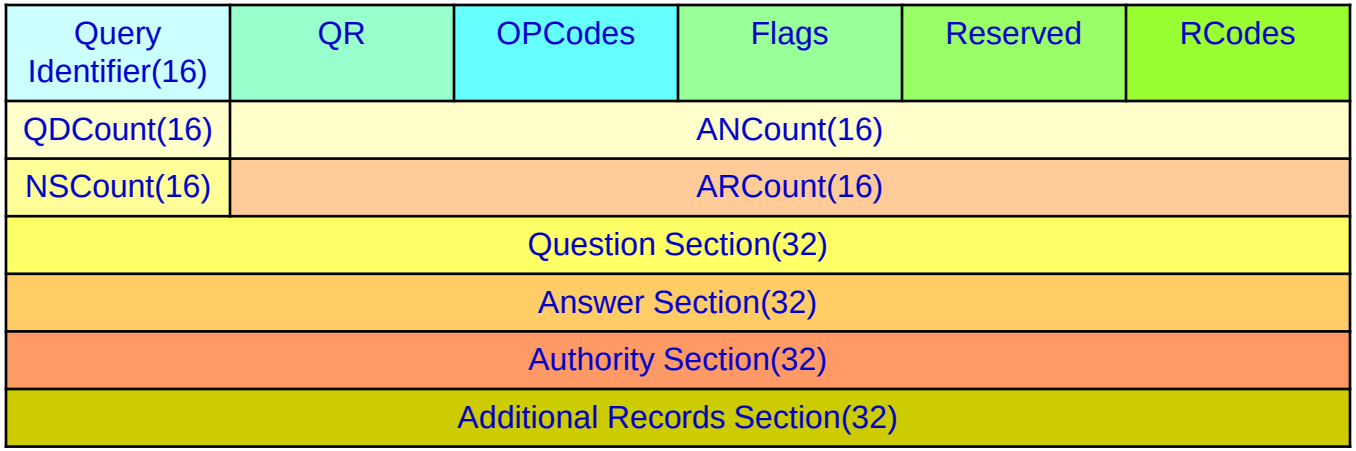

```
[root@pc071 named]# dig @211.72.211.1 xxx.com.tw ns

; <<>> DiG 8.3 <<>> @211.72.211.1 xxx.com.tw ns
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY， status: NOERROR， id: 6
;; flags: qr aa rd ra; QUERY: 1， ANSWER: 2， AUTHORITY: 0， ADDITIONAL:
   2
;; QUERY SECTION:
;;      xxx.com.tw， type = NS， class = IN

;; ANSWER SECTION:
xxx.com.tw.             1D IN NS        ns2.xxx.com.tw.
xxx.com.tw.             1D IN NS        ns1.xxx.com.tw.

;; ADDITIONAL SECTION:
ns2.xxx.com.tw.         1D IN A         211.72.211.2
ns1.xxx.com.tw.         1D IN A         211.72.211.1
```

以dig追蹤(2)

- 命令格式為

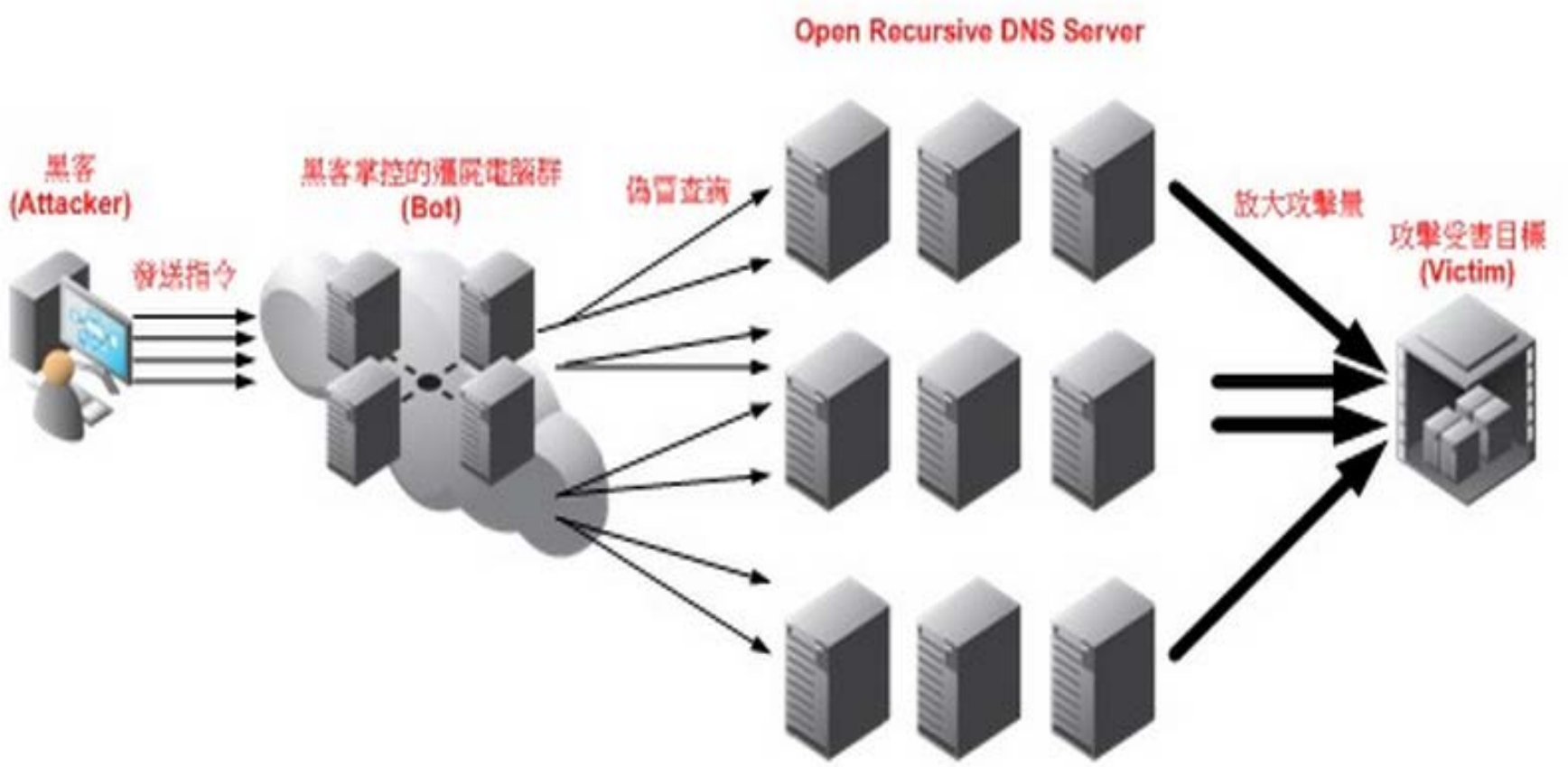
  dig @dns_server domain type

- 由上頁可看出 dig 較 nslookup 複雜許多
- 其列出許多 DNS 封包的欄位資訊，可參考 RFC 1034/1035 或 Oreilly “DNS & BIND” 一書之介紹
- DNS封包格式



DNS放大攻擊

DNS放大攻擊流程



Open Recursive DNS resolver 指 Caching recursive DNS 伺服器對外公開（不限使用對象），提供名稱遞迴解析 (recursive name resolution)服務

- 一般查詢與回應其DNS應用層訊息長度(不含UDP 標頭)分別為25 與473bytes，回應放大約為19倍
- 若查詢方式為DNSSEC ，則其查詢與回應分別為36 與1275bytes，回應放大約為35倍
- 對一部開放性DNS 解析伺服器每秒進行100 次查詢，就能產生1.02 Mbps 的攻擊流量，而攻擊者的僵屍電腦僅付出28.8 Kbps 頻寬

防治方法(Linux)

- Bind

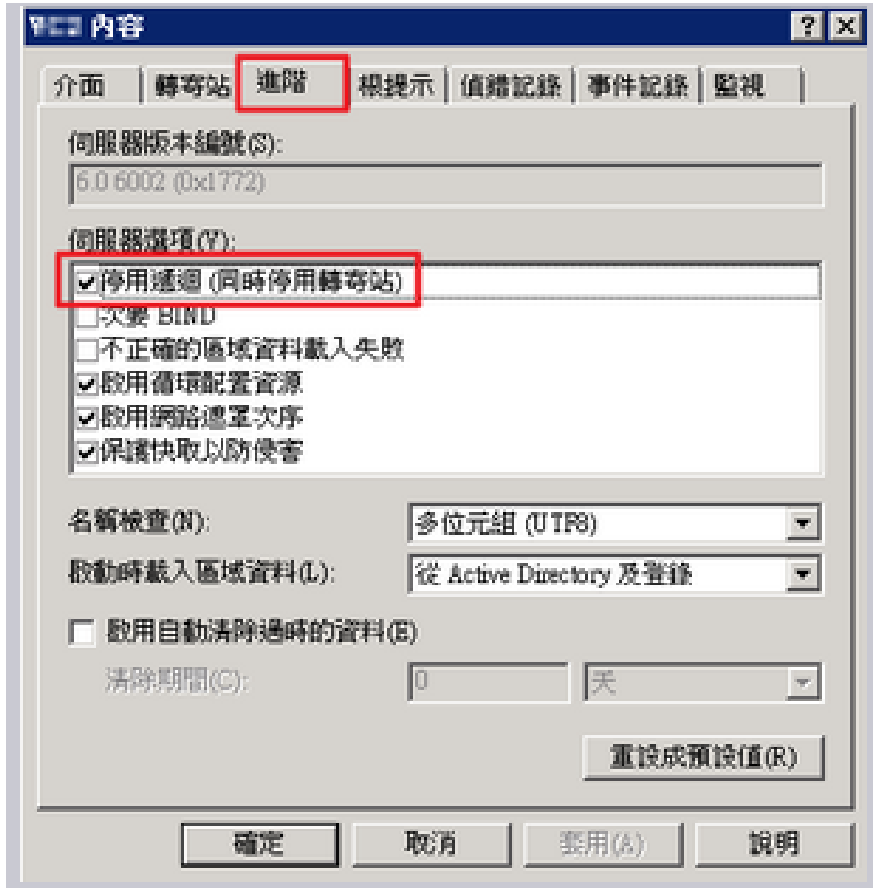
#vi /etc/named/named.conf

Options {
……
Allow-recursion { 140.113.0.0/16; };　限制可以遞迴查詢之IP
……
};

或者

Options {
……
recursion no;　關閉遞迴查詢
……
};

防治方法(Windows)



關閉DNS服務或關閉遞迴查詢

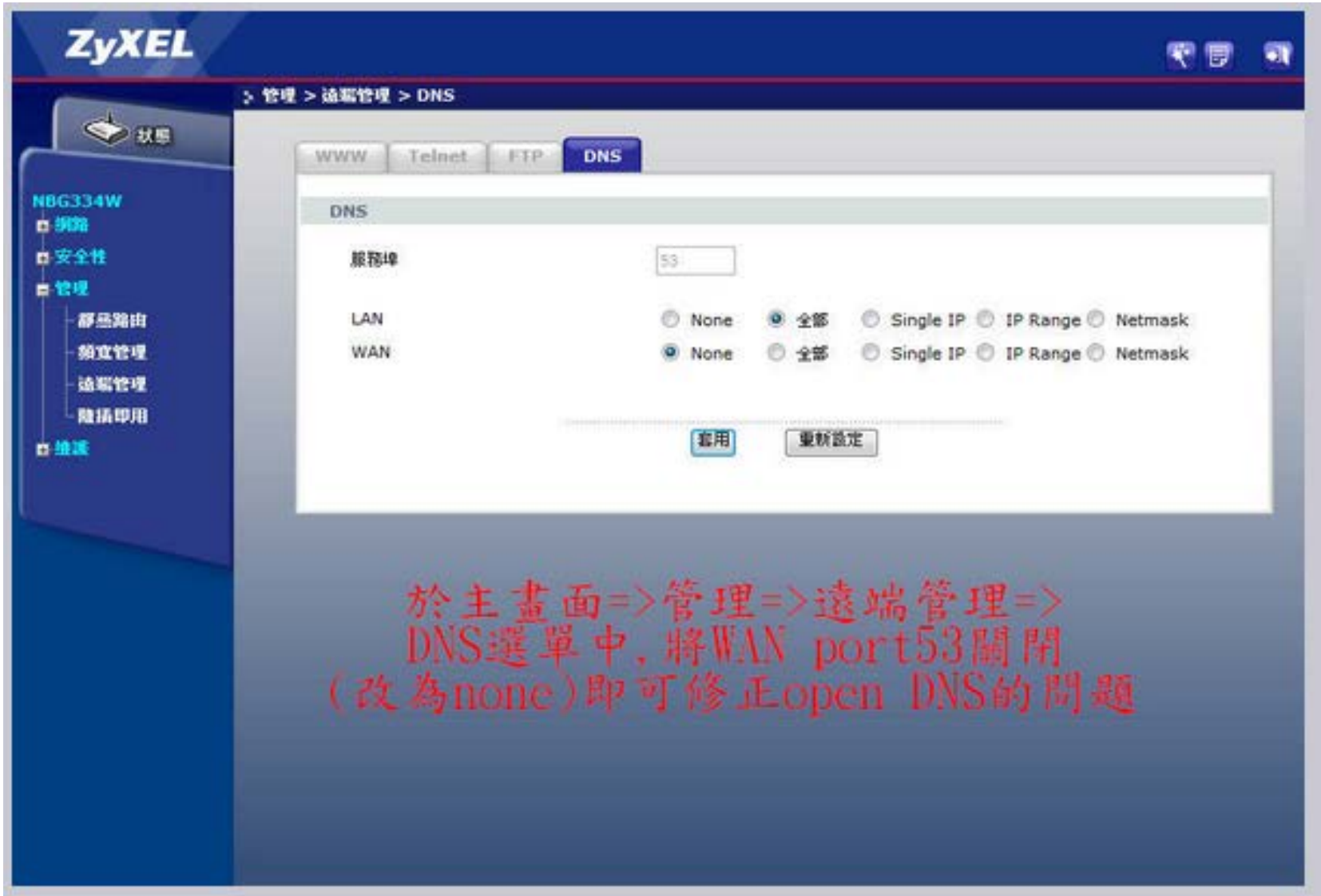
防治方法(IP分享器)


D-Link
Building Networks for People
AirPlus XTREME G™
Wireless 108G Storage Router
DI-624S
主頁
進階功能
工具
狀態
幫助
設定精靈
無線通訊
廣域網路
區域網路
DHCP伺服器
檔案分享
FTP伺服器
WEB伺服器
區域網路設定
本功能為設定 DI-624S 的區域網路端 (LAN端) IP 位址。
IP 位址
192.168.0.1
子網路遮罩
255.255.255.
0
本機網域名稱
(optional)
(可省略)
DNS Relay
啟用
停用
套用
取消
說明

防治方法(IP分享器)


dd-wrt.com ... control panel
基本設定
無線網路
伺服器
系統安全
連線限制
NAT / QoS
系統管理
機器狀態
基本設定
動態DNS (DDNS)
MAC位址複製
進階路由
網路
EoIP 通道
WAN 設定
WAN 連接類型
連接類型
靜態 IP
WAN IP位址
子網路遮罩
閘道
STP
啟用
關閉
網路設定
路由器 IP
本地IP位址
192 . 168 . 0 . 1
子網路遮罩
255 . 255 . 255 . 0
閘道
0 . 0 . 0 . 0
Local DNS
8 . 8 . 8 . 8
網路位址伺服器設定 (DHCP)
DHCP 類型
DHCP 伺服器
DHCP 伺服器
啟用
關閉
IP 開始位址
192.168.0. 100
最大 DHCP 用戶數
100
用戶端租用時間
1440 分鐘
WINS
0 . 0 . 0 . 0
Use DNSMasq for DHCP
Use DNSMasq for DNS
DHCP-Authoritative
時間設定
幫助
自動設定 - DHCP:
Cable使用者的常用選項.
主機名:
請輸入您的 ISP 提供的主機名.
網域名稱:
限制 DHCP 分配的位址數.輸入 0
配預先設定的靜態位址
時間設定:
UTC時間.
預設是啟動的

防治方法(IP分享器)


ZyXEL
管理 > 遠端管理 > DNS
狀態
NBG334W
網路
安全性
管理
靜態路由
頻寬管理
遠端管理
隨插即用
維護
WWW
Telnet
FTP
DNS
DNS
服務埠
53
LAN
None
全部
Single IP
IP Range
Netmask
WAN
None
全部
Single IP
IP Range
Netmask
套用
重新設定
於主畫面=>管理=>遠端管理=>
DNS選單中，將WAN port53關閉
(改為none)即可修正open DNS的問題

DNS 管理 – 架設篇

DNS 架 設 設 定

- Resolver(Cache Only)架設
- DNS Log設定
- 權威伺服器架設
- Master and Slave設定

課程環境資訊

- OS: Ubuntu 14.04 LTS
- 3台VM：master(10.0.2.4) 、slave(10.0.2.5)、resolver/client(10.0.2.6)
- 密碼：12345
- 3台VM可以互通，也可以透過NAT上網
- #sudo apt-get update
- #sudo apt-get dist-upgrade

Resolver架設

- #sudo apt-get install bind9 bind9-doc dnsutils
- 設定檔位置
  - /etc/bind/named.conf
  - /etc/bind/named.conf.options
  - /etc/bind/named.conf.local
- 查看bind版本
  - #named -v

BIND 9.9.5-3ubuntu0.5-Ubuntu (Extended Support Version)

Resolver架設

- 設定/etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";
        省略……..
        dnssec-validation auto;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        allow-recursion { 127.0.0.1; 10.0.2.4; };
        allow-transfer { none; };
};
```

Resolver架設

- 重新啟動
  - #sudo /etc/init.d/bind9 restart
- 檢查查詢是否正常
  - #nslookup www.google.com 127.0.0.1
- 測試從master與slave，向resolver查詢是否正常
- master#nslookup www.google.com 10.0.2.6
- slave#nslookup www.google.com 10.0.2.6

DNS Log設定

- 注意系統對於bind的log寫入目位置的設定
  - #less /etc/apparmor.d/usr.sbin.named
  - #sudo mkdir /var/log/named
  - #sudo chown -R bind:bind /var/log/named

File /etc/apparmor.d/usr.sbin.named

```
# some people like to put logs in /var/log/named/ instead of having
# syslog do the heavy lifting.
  /var/log/named/** rw,
  /var/log/named/ rw,
```

DNS Log設定

- #vi /etc/bind/named.conf.local

```
logging {
category default {default_log;};
category queries {query_log;} ;
channel default_log {
        file "/var/log/named/dns-default.log" versions 3 size 10m;
        severity info;
        print-severity yes;
        print-time yes;
   };
channel query_log {
        file "/var/log/named/dns-query.log" versions 3 size 50m;
        severity info;
        print-time yes;
   };
};
```

default : 記錄bind啟動訊息與zone傳送的狀態
query : 記錄client到此DNS查詢的記錄

DNS Log設定

- 設定完之後重新啟動bind
  - /etc/init.d/bind9 restart
- 查看/var/log/named目錄中是否有log檔產生

```
root@radius:/var/log/named# ls -al
總計 12
drwxr-xr-x  2 bind bind   4096 11月 20 08:49 .
drwxrwxr-x 10 root syslog 4096 11月 20 00:36 ..
-rw-r--r--  1 bind bind    440 11月 20 08:49 dns-default.log
-rw-r--r--  1 bind bind      0 11月 20 08:49 dns-query.log
```

權威伺服器架設

- Master：10.0.2.4
- Slave：10.0.2.5
- Client：10.0.2.6

權威伺服器架設

- Master :
  - vi /etc/bind/named.conf.local

加入:

```
zone “mydomain.edu.tw" {
        type master;
        file "/etc/bind/z.mydomain.edu.tw ";
        allow-transfer { 10.0.2.5; };
};
```

權威伺服器架設

- Slave:
  - #vi /etc/bind/named.conf.local

加入:

```
zone “mydomain.edu.tw” {
        type slave;
        masters {
        10.0.2.4;
         };
        file "/etc/bind/slave.z.mydomain.edu.tw ";
        allow-transfer { none; };
};
```

權威伺服器架設

- Master : z.mydomain.edu.tw檔案內容
  - #vi /etc/bind/z.mydomain.edu.tw

```
$TTL    3600
$ORIGIN    mydomain.edu.tw.
@       IN SOA  ns1.mydomain.edu.tw. hostmaster.mydomain.edu.tw. (
                2015060902      ; Serial Number
                1800            ; Refresh  30M
                900             ; Retry      15M
                604800          ; Expire    7D
                604800 )        ; Minimum

              IN      NS   ns1.mydomain.edu.tw.
              IN      NS   ns2.mydomain.edu.tw.
ns1             IN      A       10.0.2.4
ns2             IN      A       10.0.2.5
www             IN      A       140.126.180.41
docs            IN      CNAME   ghs.google.com.
ftp           900 IN     A       10.0.2.100
```

權威伺服器架設

- 重新啟動master與slave bind
  - Master : #/etc/init.d/bind9 restart
  - Slave : #/etc/init.d/bind9 restart

權威伺服器架設

- 檢查slave是否有收到master傳過來的zone
  - Slave : #less /etc/bind/slave.z.mydomain.edu.tw
  - Slave有看到slave.z.mydomain.edu.tw檔案，內容序號正確，代表zone transfer正常

權威伺服器架設

- 使用client(10.0.2.6)去查詢zone的內容，看看回覆的內容
  - #nslookup ftp.mydomain.edu.tw 10.0.2.4
  - #nslookup ftp.mydomain.edu.tw 10.0.2.5
  - #nslookup www.google.com 10.0.2.4
  - #dig @10.0.2.5 soa mydomain.edu.tw
  - #dig @10.0.2.4 ns mydomain.edu.tw

權威伺服器架設

- #dig @10.0.2.5 ftp.mydomain.edu.tw
- #dig @10.0.2.5 www.mydomain.edu.tw
- check以上的TTL

Q & A

謝謝