DomainNameSystem

蔡政道

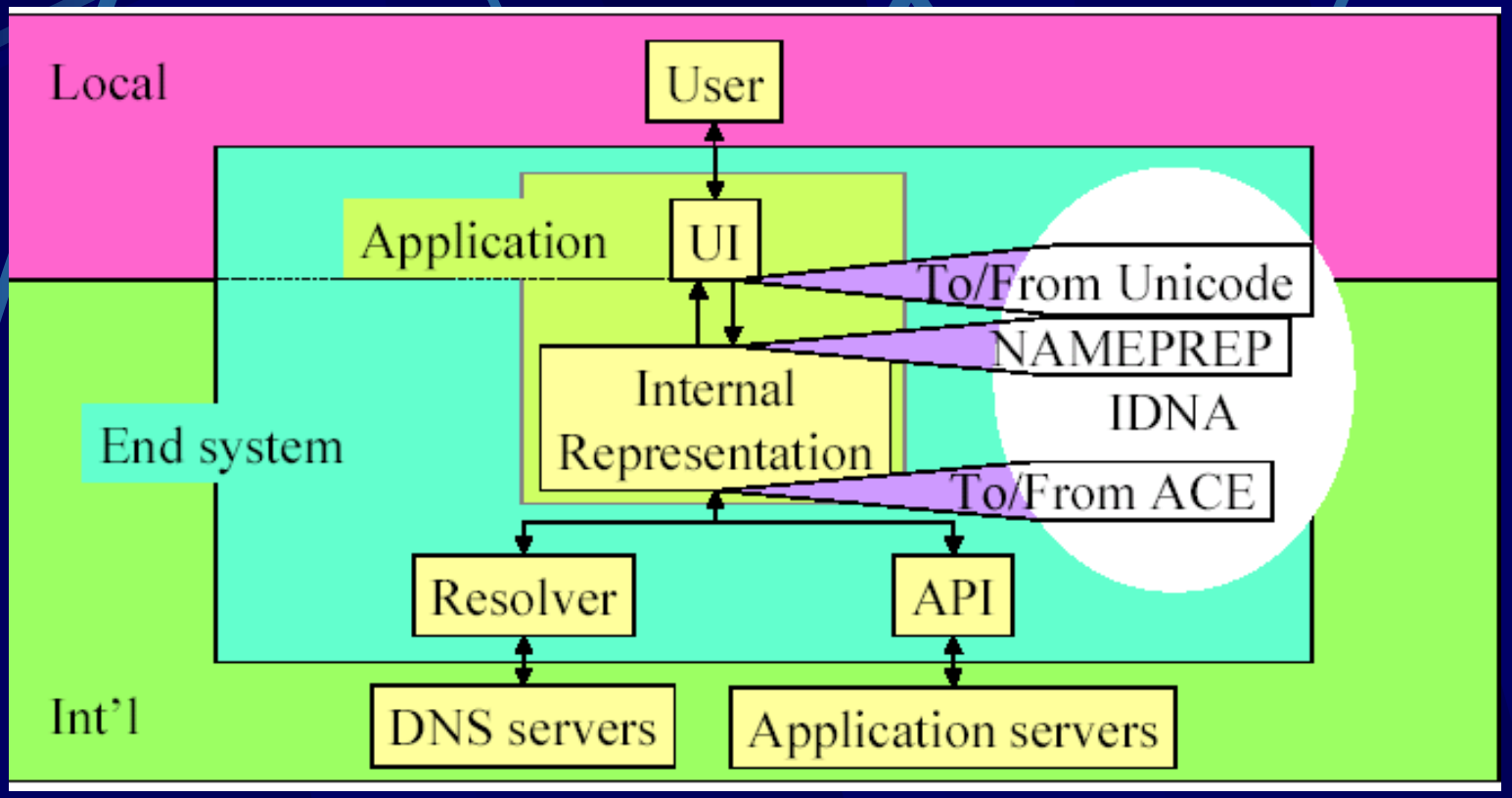
Ver.921124

- 網域名稱是電腦在網路上的身份，
  - 如同 IP 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
  - 隨著 Internet 及 IPv6 的發展，網域名稱的作用將更顯得重要

中文網域名稱之優點

- 優點
  - 就國人而言中文字較英文字好記
    總統府　=> http://www.president.gov.tw/
    中文域名 => http://總統府.tw/
  - 能和企業名稱一致
    統一企業 =>http://www.uni-president.com.tw/
    中文域名 => http://統一企業.tw

國際域名(IDN)標準


Local
User
Application
UI
To/From Unicode
NAMEPREP
IDNA
Internal
Representation
End system
To/From ACE
Resolver
API
Int'l
DNS servers
Application servers

國際域名(IDN)標準

- 中文字應透過某種編碼方式轉換成英文字，並與舊有的 DNS 系統相容
- DNS 設定及伺服器設定應都根據這個編碼定義
- 目前國際上認可的編碼為 AMC-ACE-Z，稱為 puny code (RFC 3492)

例:

http://xn--fiq43lrrlz83a.tw/ 台網中心.tw
http://xn--fiq64bh55hj6p.tw/ 中華電信.tw
http://xn--nqq28iuws7nz.tw/ 數位聯合.tw
http://xn--pssu7c921afvu.tw/ 清華大學.tw

域名之分類

- 分類: 在區分不同的屬性
  - Top Level Domain (TLD) 頂級域名
    - gTLDs:
      - com/net/org/gov/edu/… 共13類
    - ccTLDs:
      - tw/cn/jp/us 共 243 個
  - Second Level Domain (第二層域名)
    - com.tw/org.tw/ 等
- 目前 tw 之第二層域名
  - com.tw/net.tw/org.tw/edu.tw/gov.tw/mil.tw
  - idv.tw/game.tw/club.tw/ebiz.tw

- 為 Internet 服務最基礎的一環
- 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
- 隨著 IPv6 (16 bytes) 的推展，更需要使用網域名稱

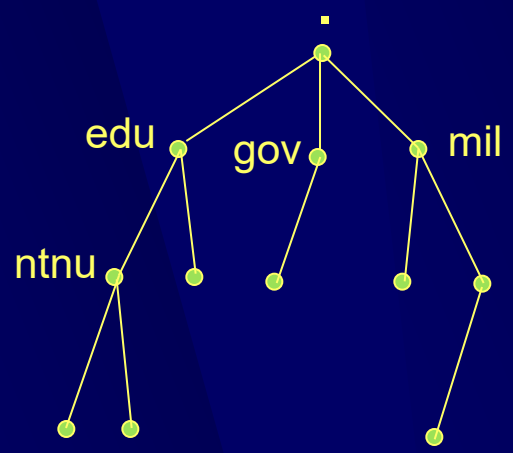
- DNS 的歷史
  - IP
  - hosts 檔
    - 網路流量與負載
    - 主機名稱的衝突
    - 資訊的一致性
- 1984年Paul Mockapetris 建立了第一個 DNS 的規範(RFC1034， RFC1035)

- DNS 是一個分散式資料庫系統(distributed database)
- 自己的資料由自己維護，而其他人的資料則分散在全球，沒有一台電腦會有全部的DNS資料
- Name Server維護整個Database中的部份資料
- Name Server提供Client(Resolver)查詢服務
- Resolver只是一些library routines, 負責透過網路向Name Server查詢資料

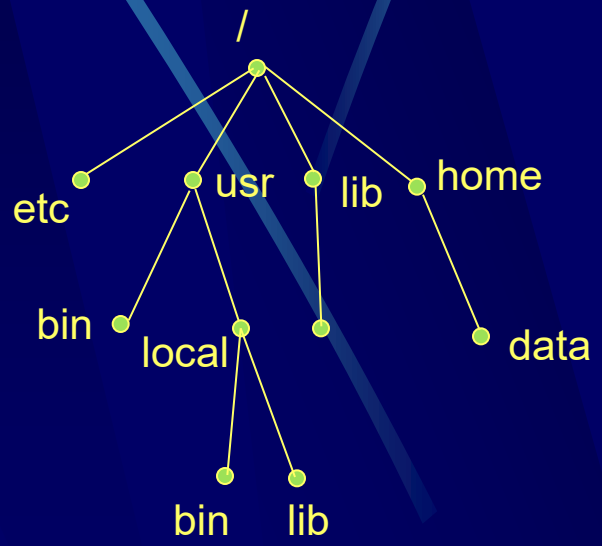
- Domain Name System is a database of hostinformation
- Domain Name可看成到DNS Database中找資料的索引(index)
- 每一個Domain在整個DNS中有唯一的名稱(Name)
- Domain Name Space is a invert tree
- 以樹狀結構的方式找到目的位址
- Domain Name指出其在整個DNS中的位置
- Each domain name is a path in the invert tree
- 負載平衡:可由 Master 主機自由的複製到 Slave 主機
- 備援:一個網域可有多台主機共同服務

- DNS資料庫的架構與UNIX的檔案系統極為類似

DNS Database

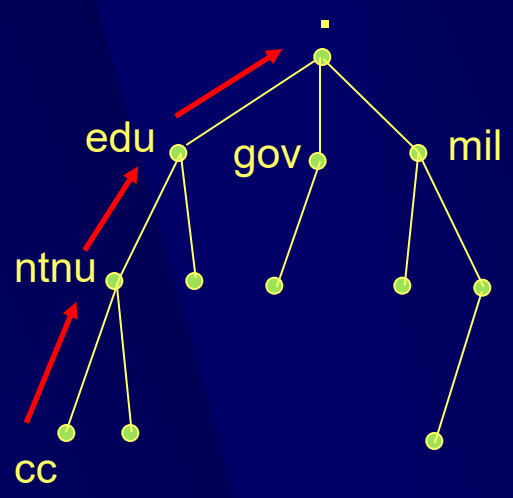


UNIX Filesystem



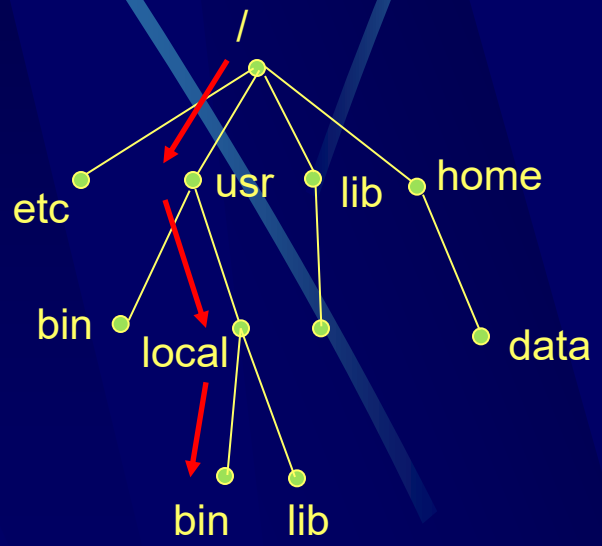
- Domain Name與UNIX Filesystem表示順序相反

DNS Database



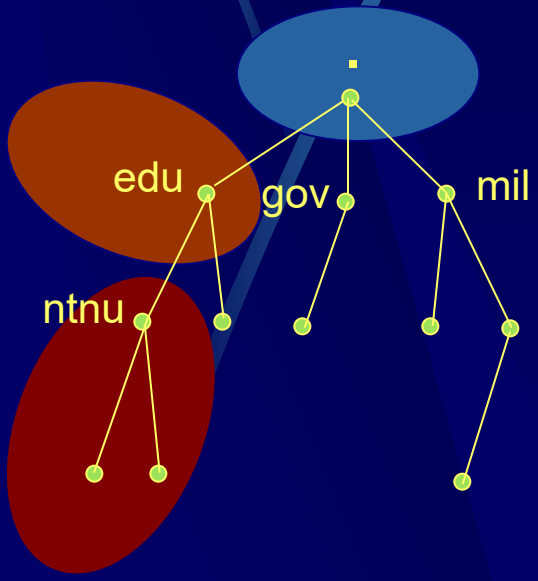
cc.ntnu.edu.

UNIX Filesystem

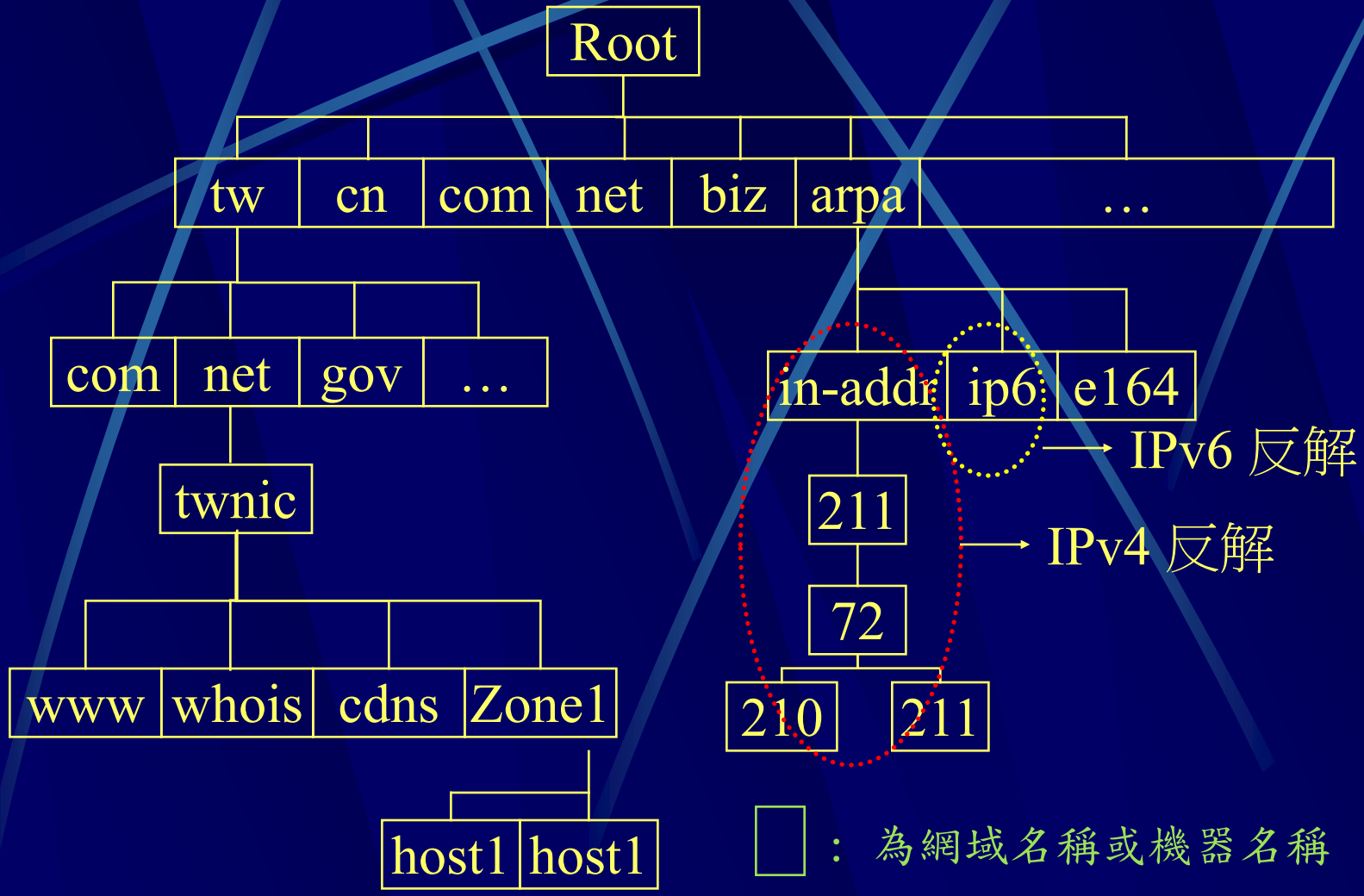


/usr/local/bin

- 每一個Domain可再分割成數個SubDomain
- 每一個SubDomain可由不同的單位維護其資料



DNS 樹狀結構


Root
tw
cn
com
net
biz
arpa
…
com
net
gov
…
twnic
www
whois
cdns
Zone1
host1
host1
in-addr
ip6
e164
IPv6 反解
211
IPv4 反解
72
210
211
：為網域名稱或機器名稱
：為上一層與下一層的委任關係
註：DNS 的搜尋由上往下

- Domain中可包含Host與SubDomain
- 每一個Host都會有一個Domain Name或多個別名(Domain Name Alias)

- The depth of the tree is limited to 127 levels
- 每一個node的名稱(text label)最多可以有63個字元
- Root的label為null(長度為0)
- Full Domain Name:
  - The sequence of labels on the path from that node to the root.

FQDN

- An absolute domain name is written relative to the root and unambiguously specifies a node's location in the tree.
- An absolute is also referred to as a Full Qualified Domain Name(FQDN)

- DNS要求相鄰的node(sibling node)(相同parent node)其label必須不同-
  - 確保每一node在tree中之domain name唯一

- Domain:
  - A subtree of domain name space
- 一個Domain的Domain Name就是這個Domain最高節點(node)的Domain Name
- 同一個Domain中的host在邏輯上彼此相關,可以是地域上,或組織上...相關;但與其IP Address,在何Network...無關

- Leaves of the tree 之Domain Name代表一個host,並指出此host的Address, Mail Routing等資訊
- Tree中的節點(interior node)可代表一host, 亦可指出此Domain的資訊
  - hp.com代表HP公司的Domain Name, 且是網路上一台host

小範圍 → 大範圍

www.slhs.tp.edu.tw.

大範圍 ← 小範圍

203.72.185.3

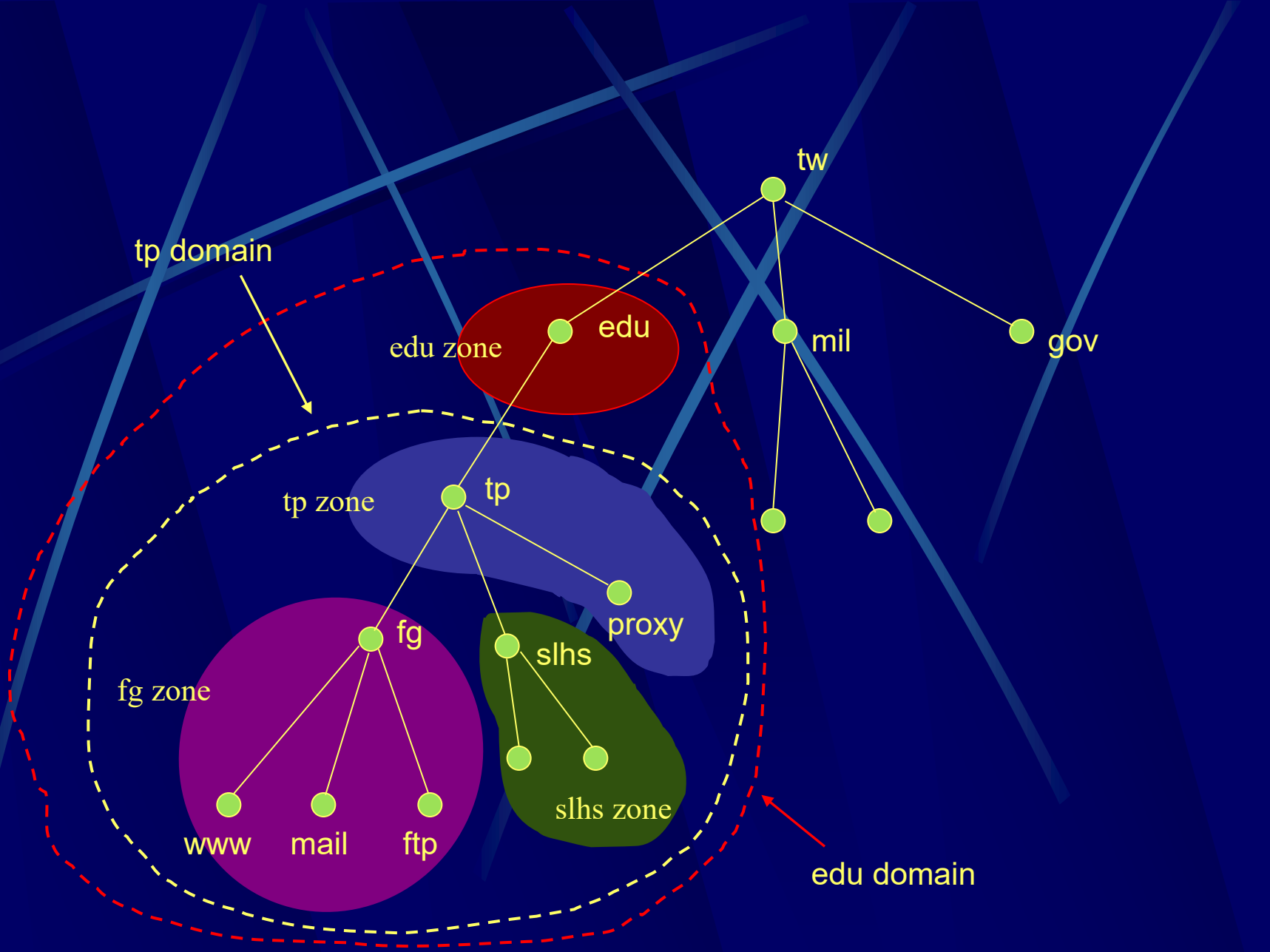
網域授權關係

- 網域名稱的管理者可以建立不同的子網域給不同的部門或單位使用
- 其亦可將此子網域授權他部門自行管理
- 在上一層的網域需指出這種授權的關係
- 整個 DNS 樹狀結構即是依此完成

Name Servers and Zones

- Name Server
  - The program that store information about the domain name space.
- Zone
  - The part of the domain name space.
  - 一個domain可切割成數個SubDomain,這些SubDomain可被授權(delegation)由其它單位管理,這些SubDomain稱為Zone

- 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.


tw
tp domain
edu
edu zone
mil
gov
tp zone
tp
proxy
fg
slhs
fg zone
slhs zone
www
mail
ftp
edu domain

Zone Data Files

- The files which primary master name servers load their zone data.
- The data files contain resource records that describe the zone.
- The resource records describe all the hosts in the zone and mark any delegation of subdomains.

Resolvers

- Clients that access name servers
- Querying a name server
- Interpreting responses
- Returning the information to the programs that requested it
- 在BIND中,並不是單獨的process,而是一library

Query Type - recursive

- The name server repeats the same basic process until it receives an answer.

Query Type - 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

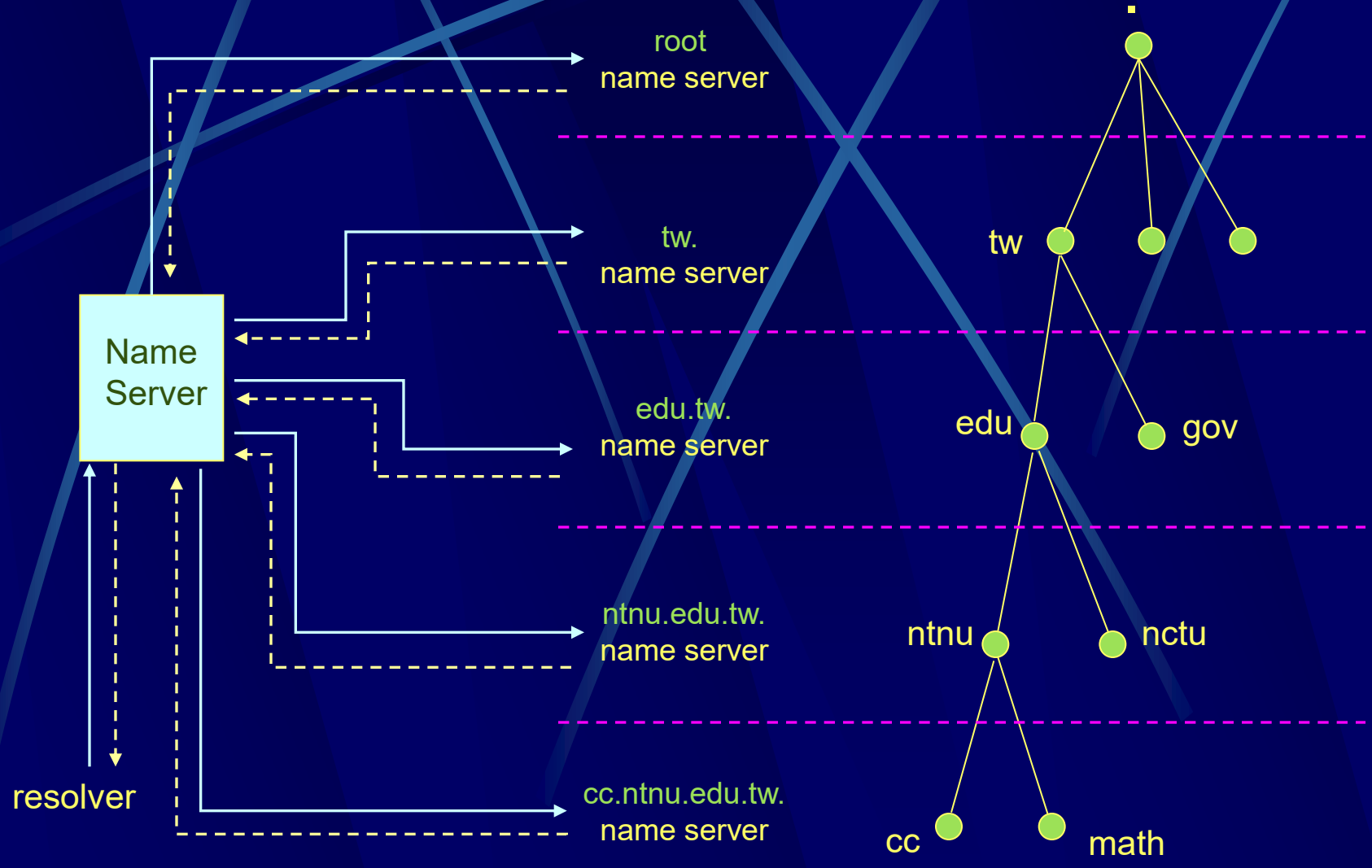
運作原理

- 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

運作原理

- 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

Query: sun3.cc.ntnu.edu.tw



DNS解析流程(1)

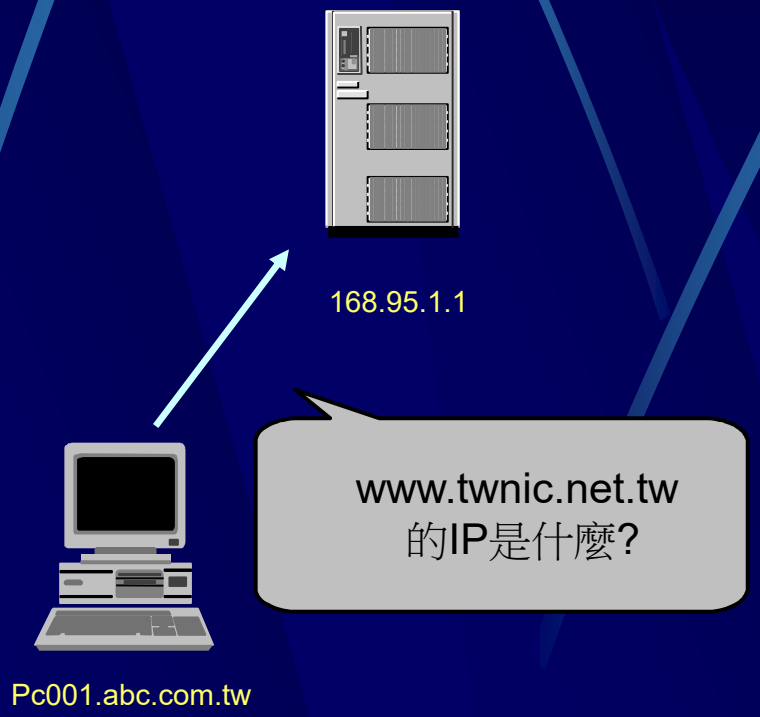
- 讓我們一步一步來看DNS解析的步驟:

Pc001.abc.com.tw

```
ping www.twnic.net.tw.
```

DNS解析流程(2)

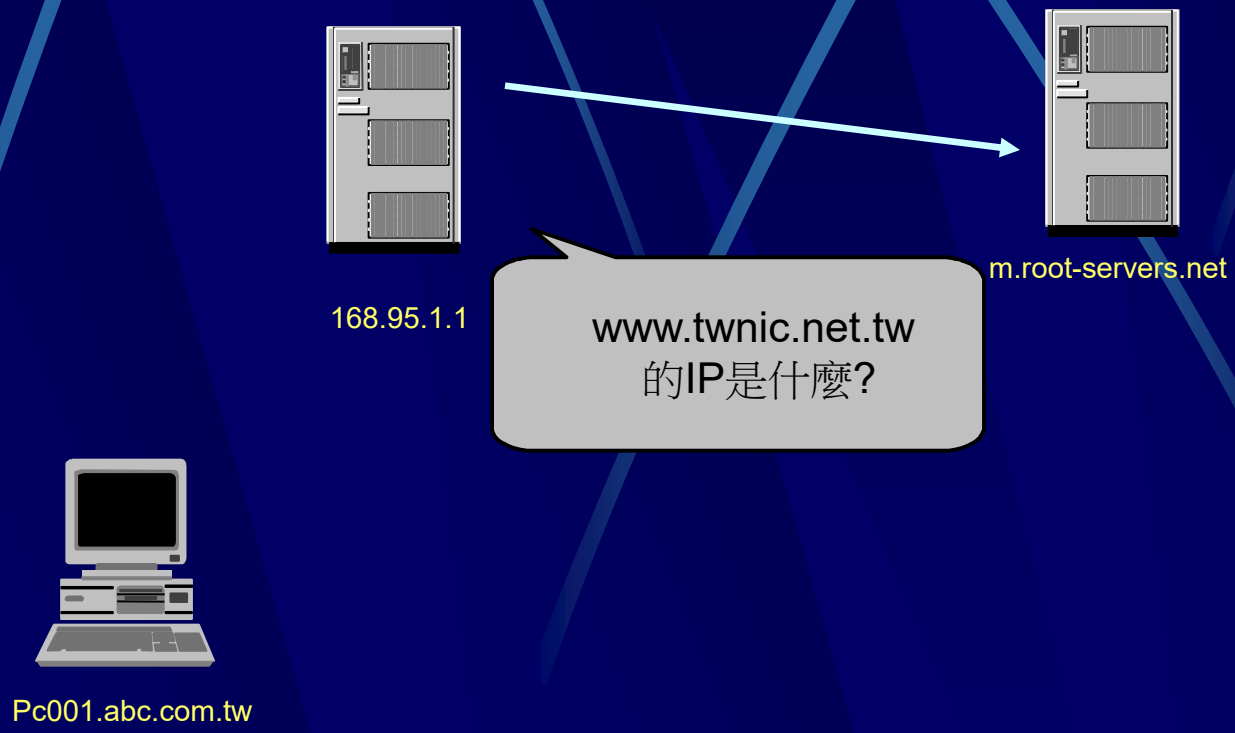
- 個人電腦向他設定的DNS 168.95.1.1查詢www.twnic.net.tw的IP




```
ping www.twnic.net.tw.
```

DNS解析流程(3)

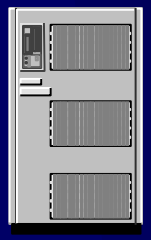
- 168.95.1.1會向root server M查詢www.twnic.net.tw的IP address



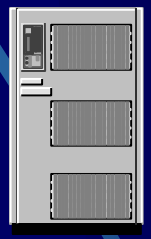
ping www.twnic.net.tw.

DNS解析流程(4)

- M root server會回應 .TW 的dns在那裡



168.95.1.1



m.root-servers.net

這裡有 .TW DNS的清單，請向其中之一查詢.

Pc001.abc.com.tw

```
ping www.twnic.net.tw.
```

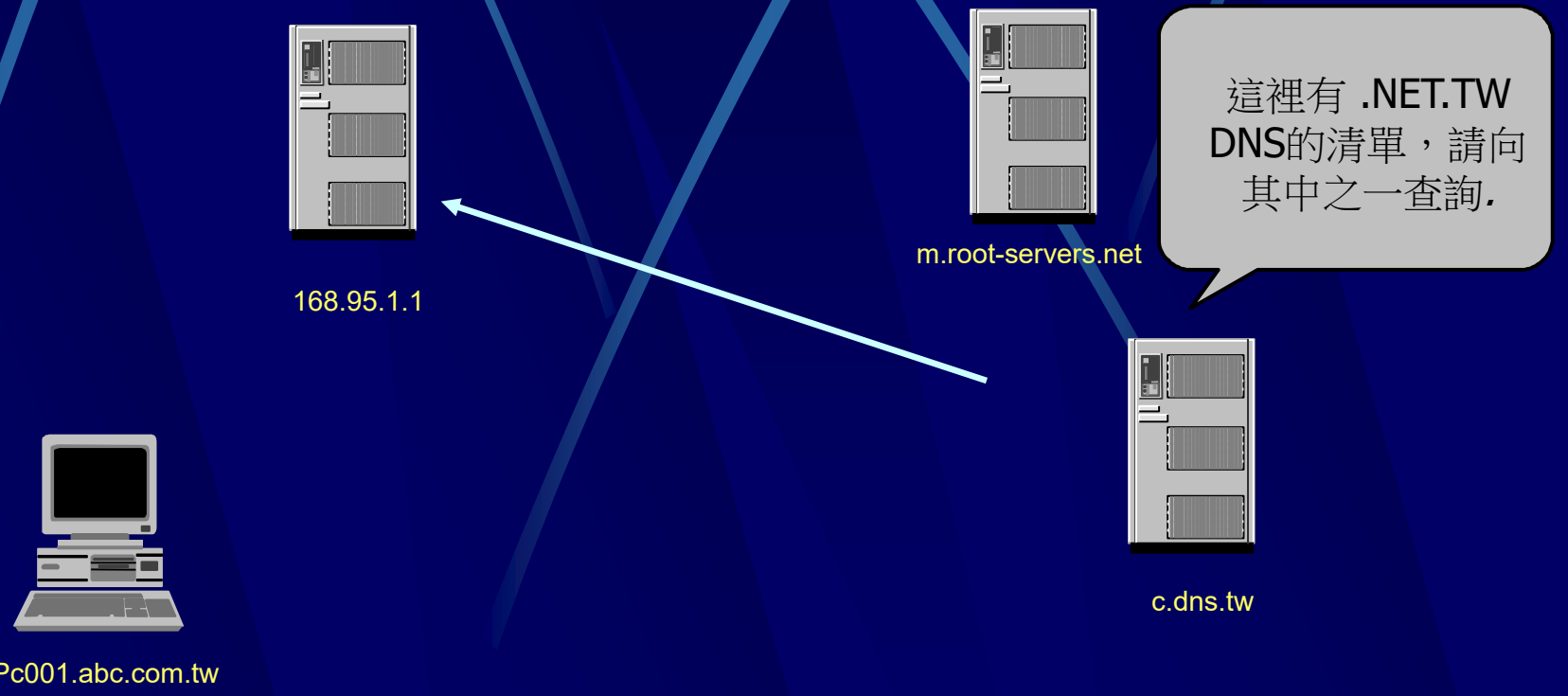
DNS解析流程(5)

- 168.95.1.1會向.TW name server: c.dns.tw查詢www.twnic.net.tw的IP address


```
ping www.twnic.net.tw.
```

DNS解析流程(6)

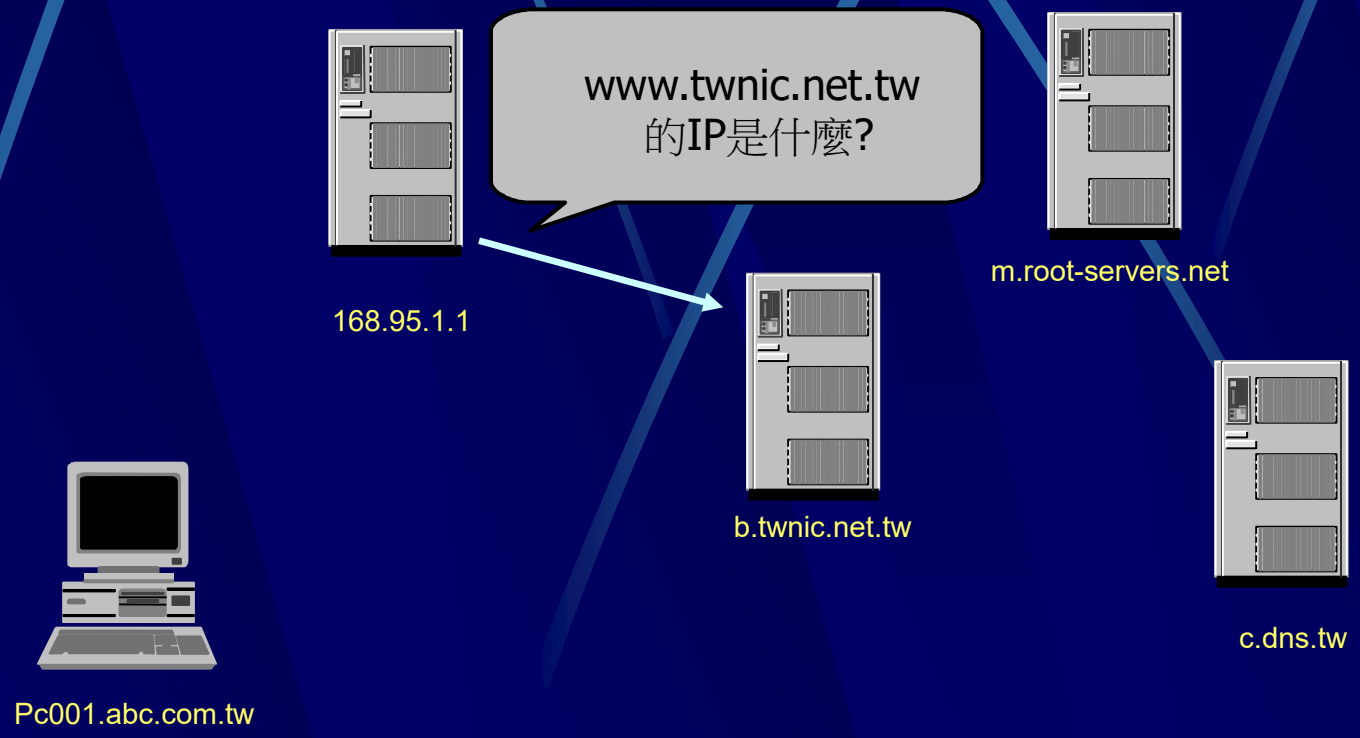
- c.dns.tw回應net.tw的DNS在那裡




```
ping www.twnic.net.tw.
```

DNS解析流程(7)

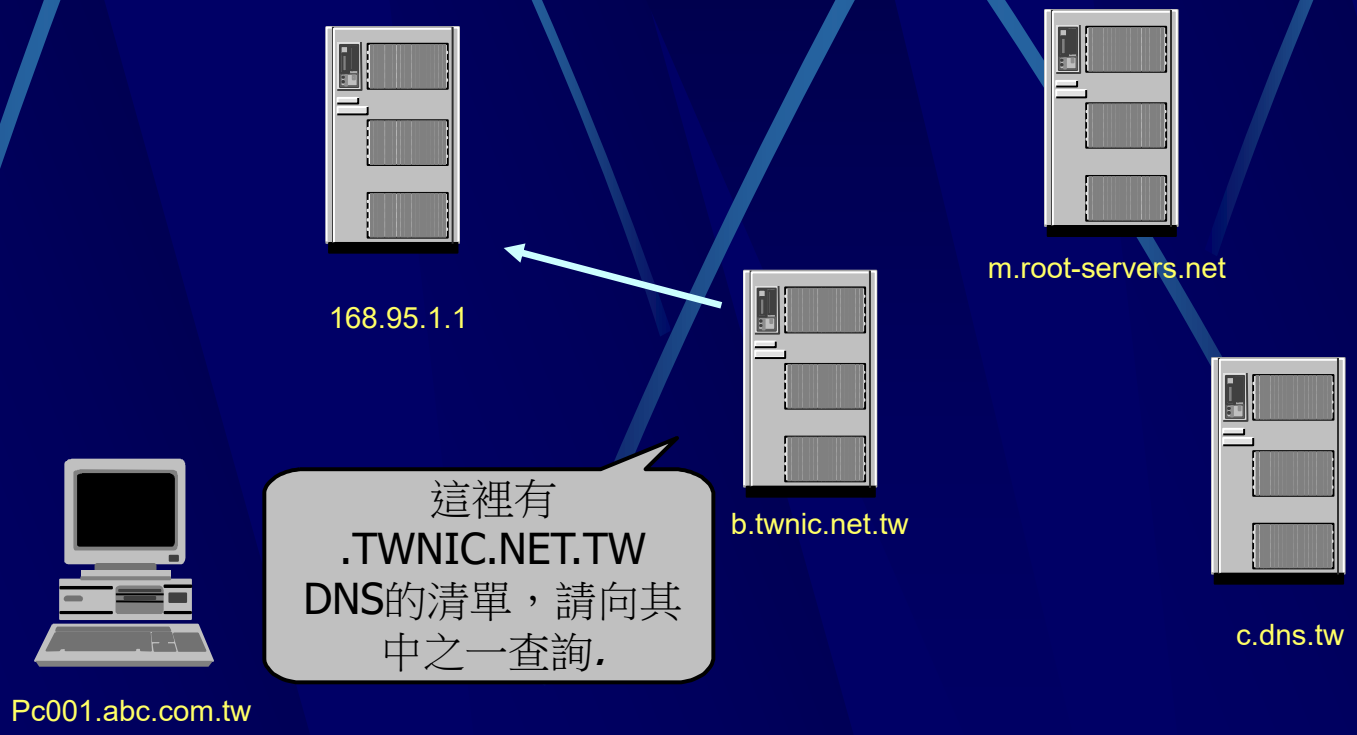
- 168.95.1.1會向.TW name server: b.twnic.net.tw查詢www.twnic.net.tw的IP address




```
ping www.twnic.net.tw.
```

DNS解析流程(8)

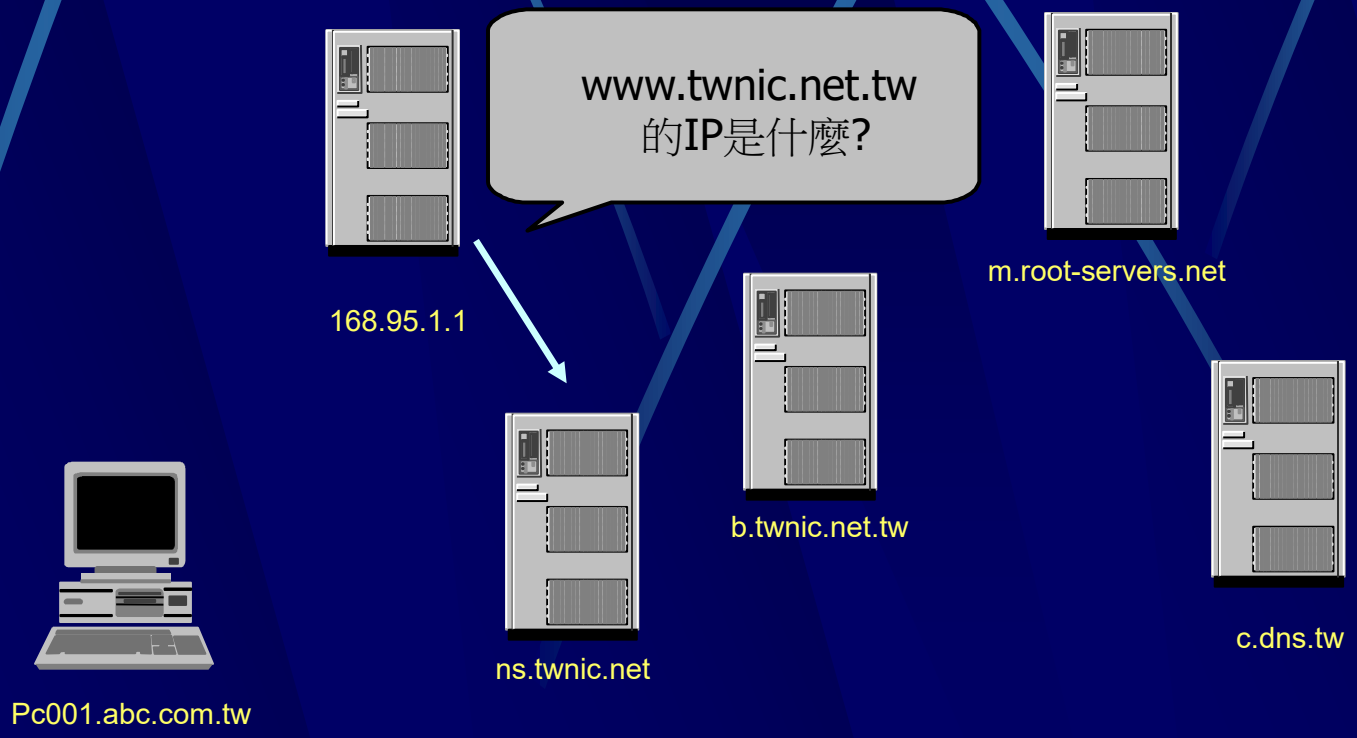
- b.twnic.net.tw回應twnic.net.tw的DNS在那裡




```
ping www.twnic.net.tw.
```

DNS解析流程(9)

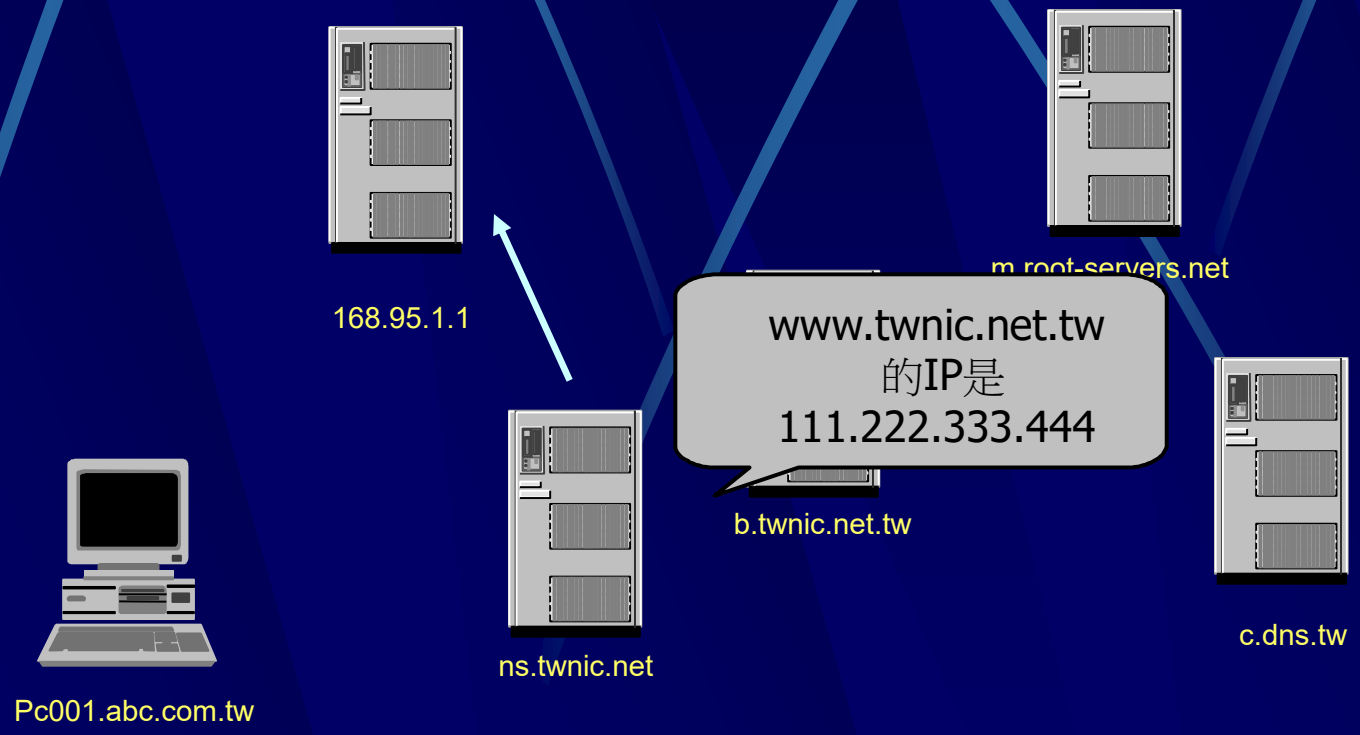
- 168.95.1.1會向ns.twnic.net查詢www.twnic.net.tw的IP address




```
ping www.twnic.net.tw.
```

DNS解析流程(10)

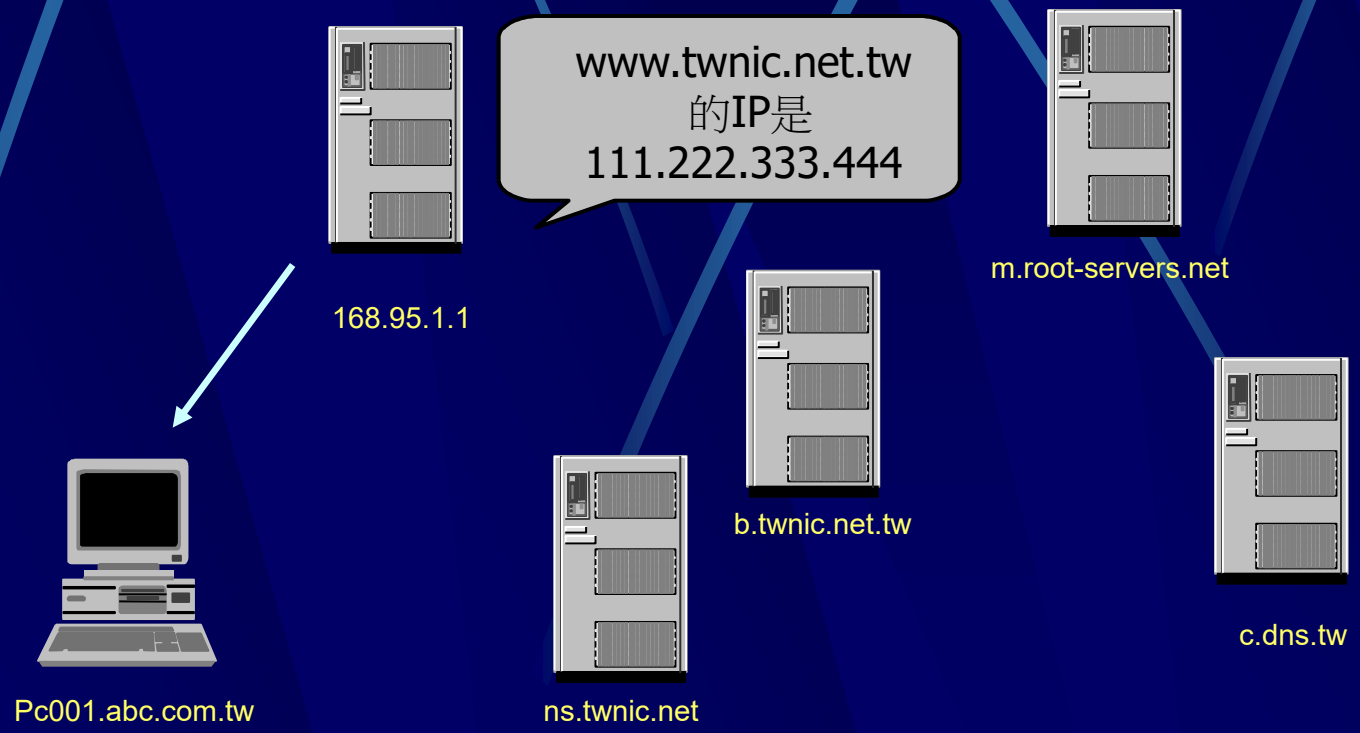
- ns.twnic.net回應www.twnic.net.tw的IP是什麼




```
ping www.twnic.net.tw.
```

DNS解析流程(11)

- 168.95.1.1回應pc001.abc.com.tw www.twnic.net.tw的IP是111.222.333.444




```
ping www.twnic.net.tw.
```

DNS解析流程Caching(1)

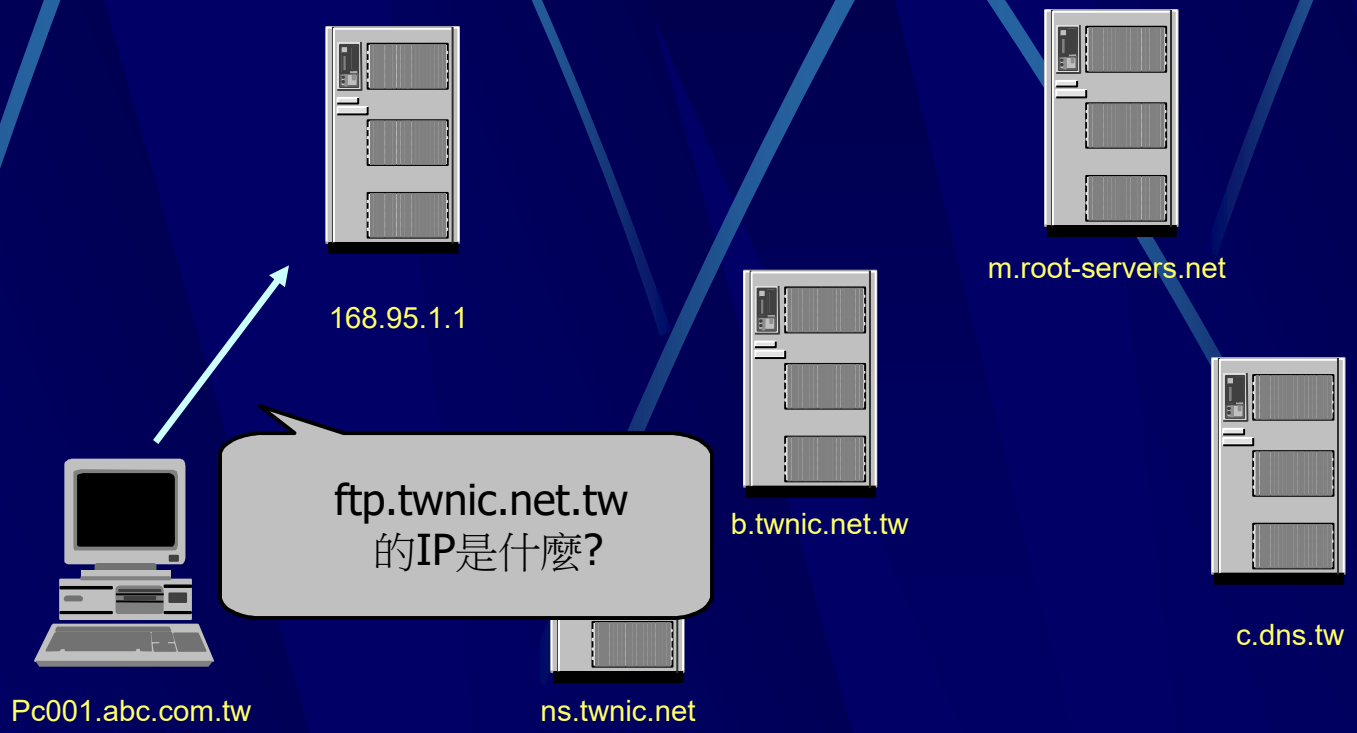
- 在前次查詢後168.95.1.1知道了下列紀錄:
  - TW的dns及其IP
  - NET.TW的dns及其IP
  - TWNIC.NET.TW的dns及其IP
  - WWW.TWNIC.NET.TW的IP
- 讓我們看下一次的解析流程

Pc001.abc.com.tw

```
ping ftp.twnic.net.tw.
```

DNS解析流程Caching(2)

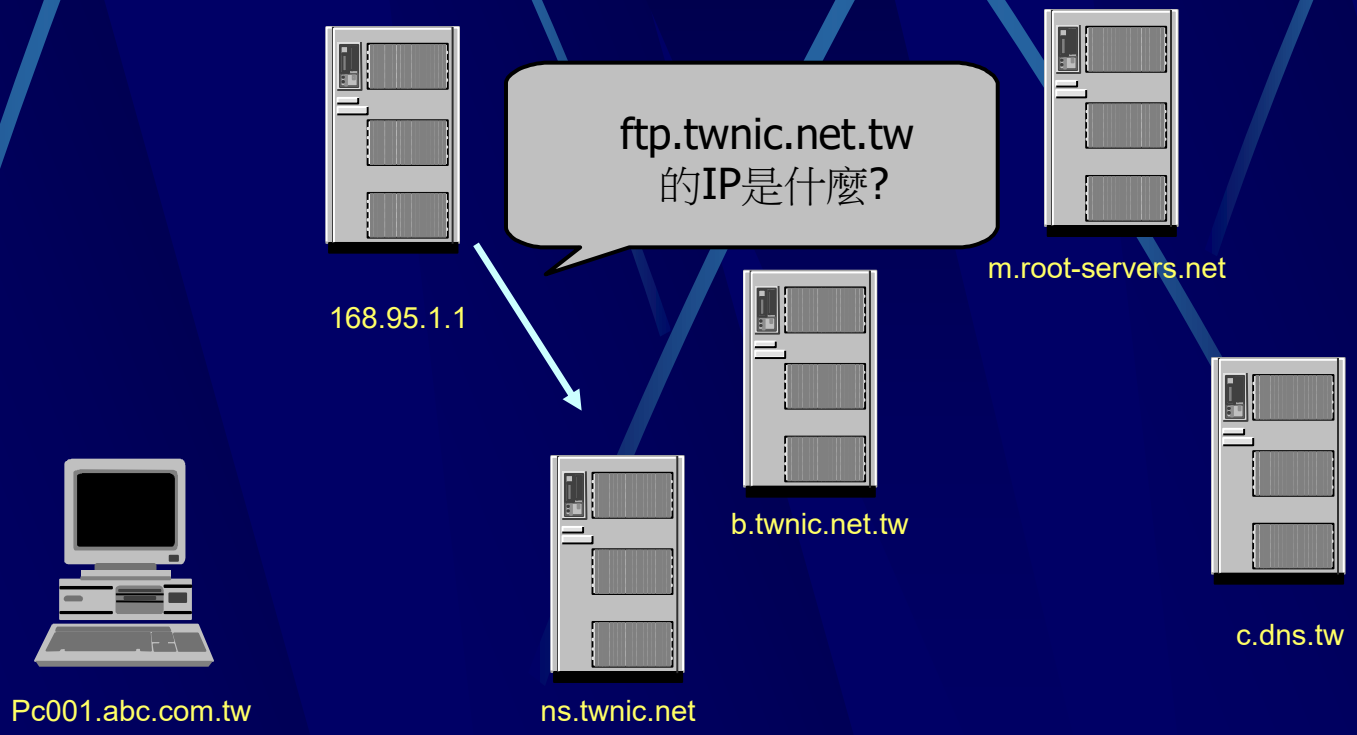
- 個人電腦向他設定的DNS 168.95.1.1查詢ftp.twnic.net.tw的IP



ping **ftp**.twnic.net.tw.

DNS解析流程Caching(3)

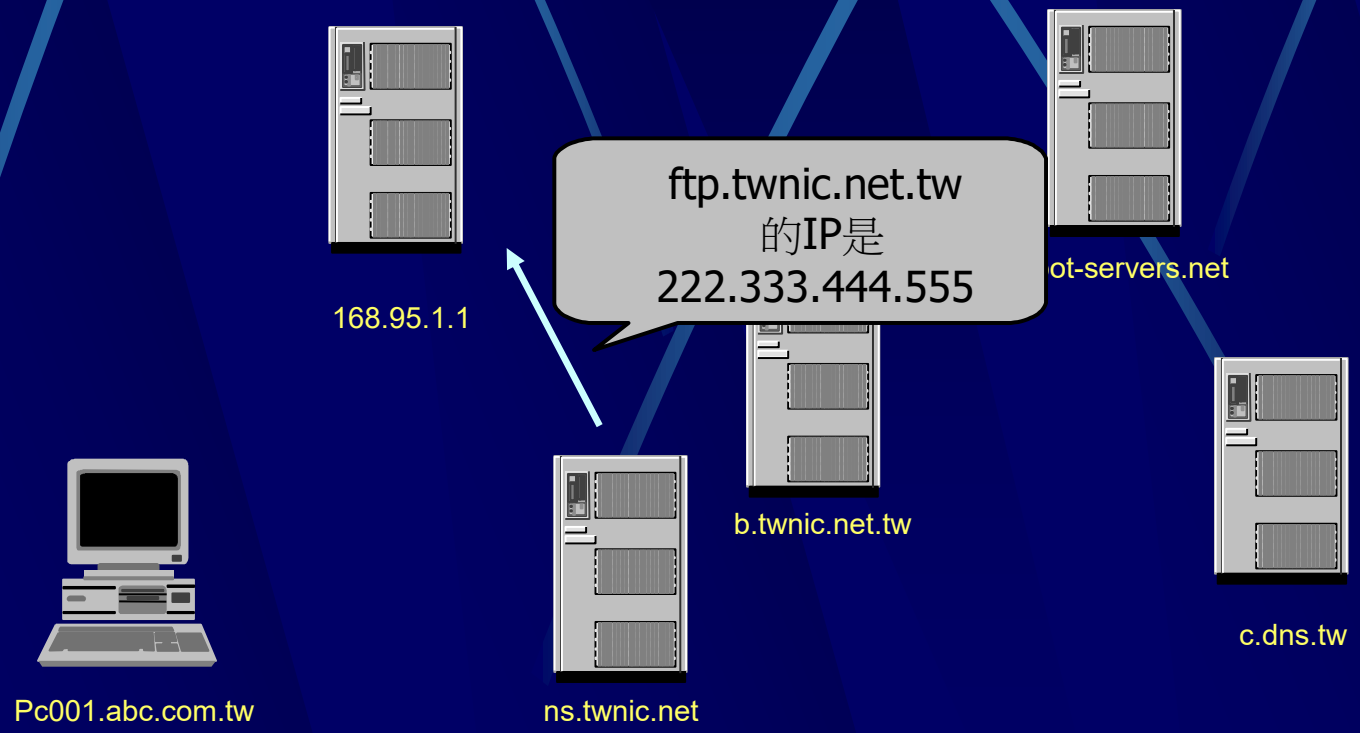
- 168.95.1.1已經有twnic.net.tw的NS紀錄， 所以直接過去詢問ftp.twnic.net.tw的IP



ping **ftp**.twnic.net.tw.

DNS解析流程Caching(4)

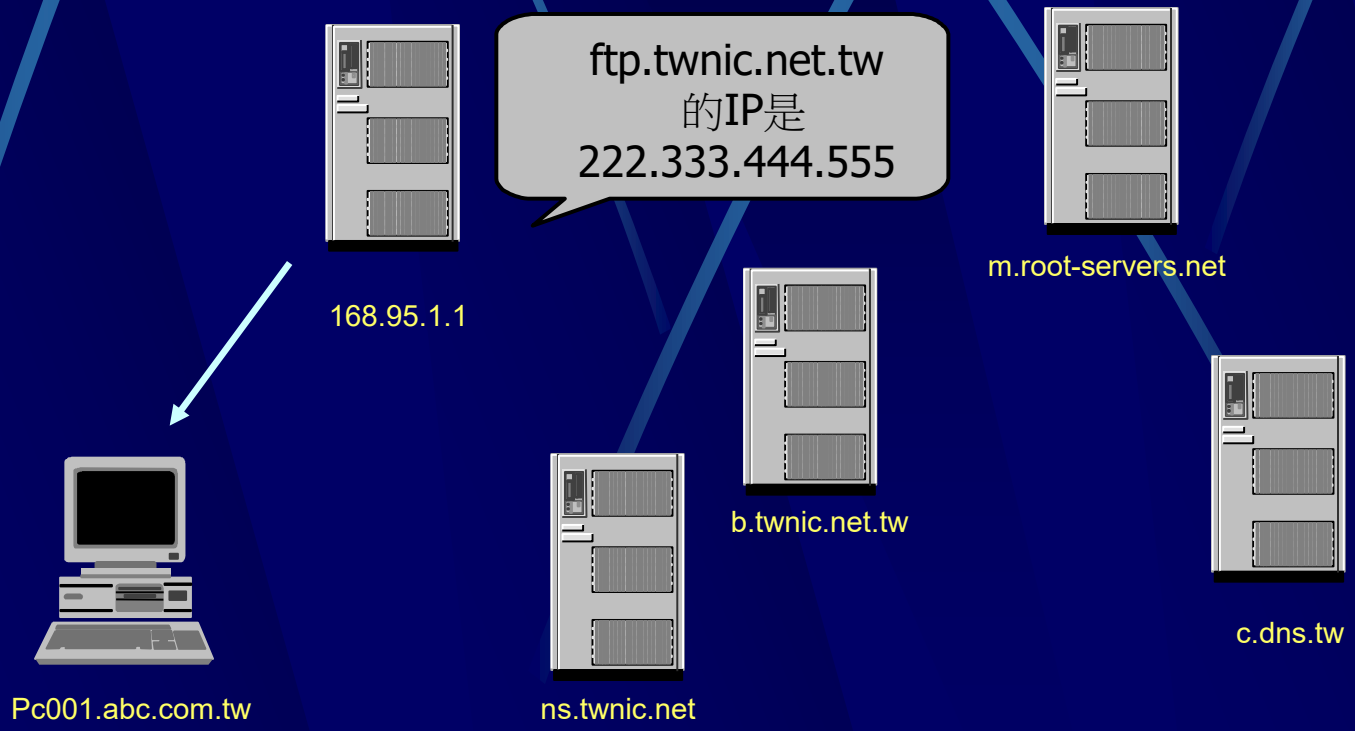
- ns.twnic.net回應ftp.twnic.net.tw的IP是什麼



ping **ftp**.twnic.net.tw.

DNS解析流程Caching(5)

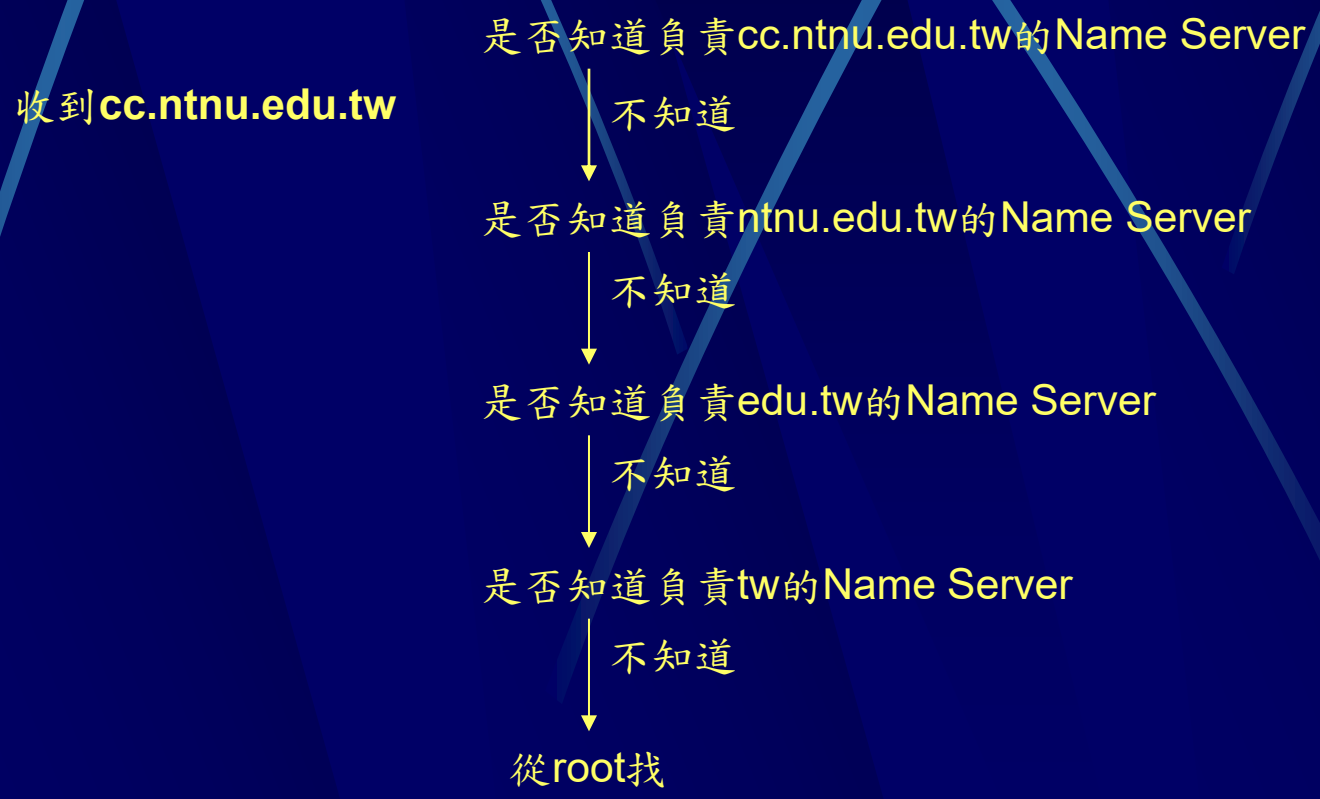
- 168.95.1.1回應pc001.abc.com.tw ftp.twnic.net.tw的IP是222.333.444.555



ping **ftp**.twnic.net.tw.

- Caching –
  - Name server將查詢過程所得到的資訊暫存起來
  - 亦會cache negative資料
- TTL(Time to Live) –
  - The amount of time that name server is allowed to cache the data

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



Choosing between authoritative name servers

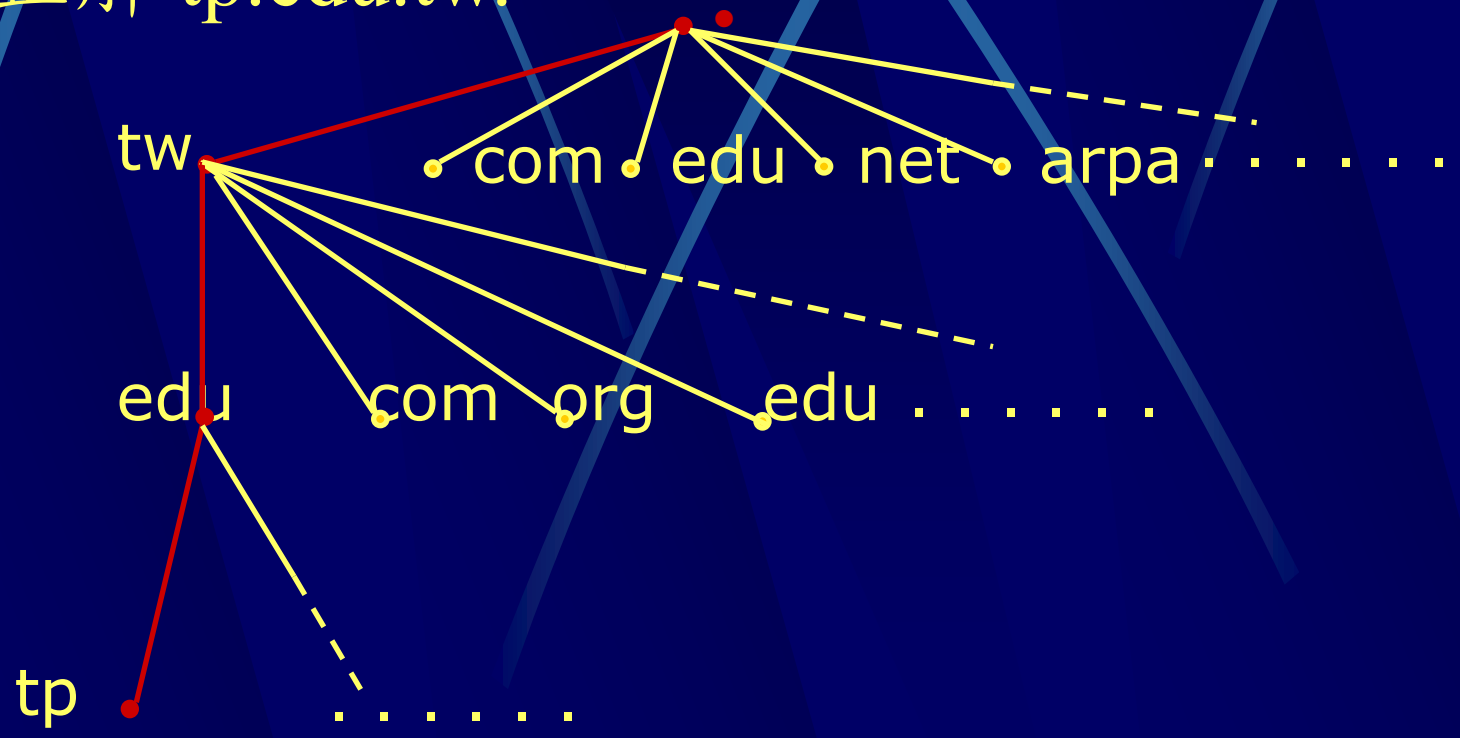
- 對同一Zone, 可能有多個authoritative name server
- 使用RoutdTrip Time(RTT)應向何name server詢問
- RTT is a measurement of how long a remote name server takes to respond to queries.

正解/反解之意義與原理

- 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

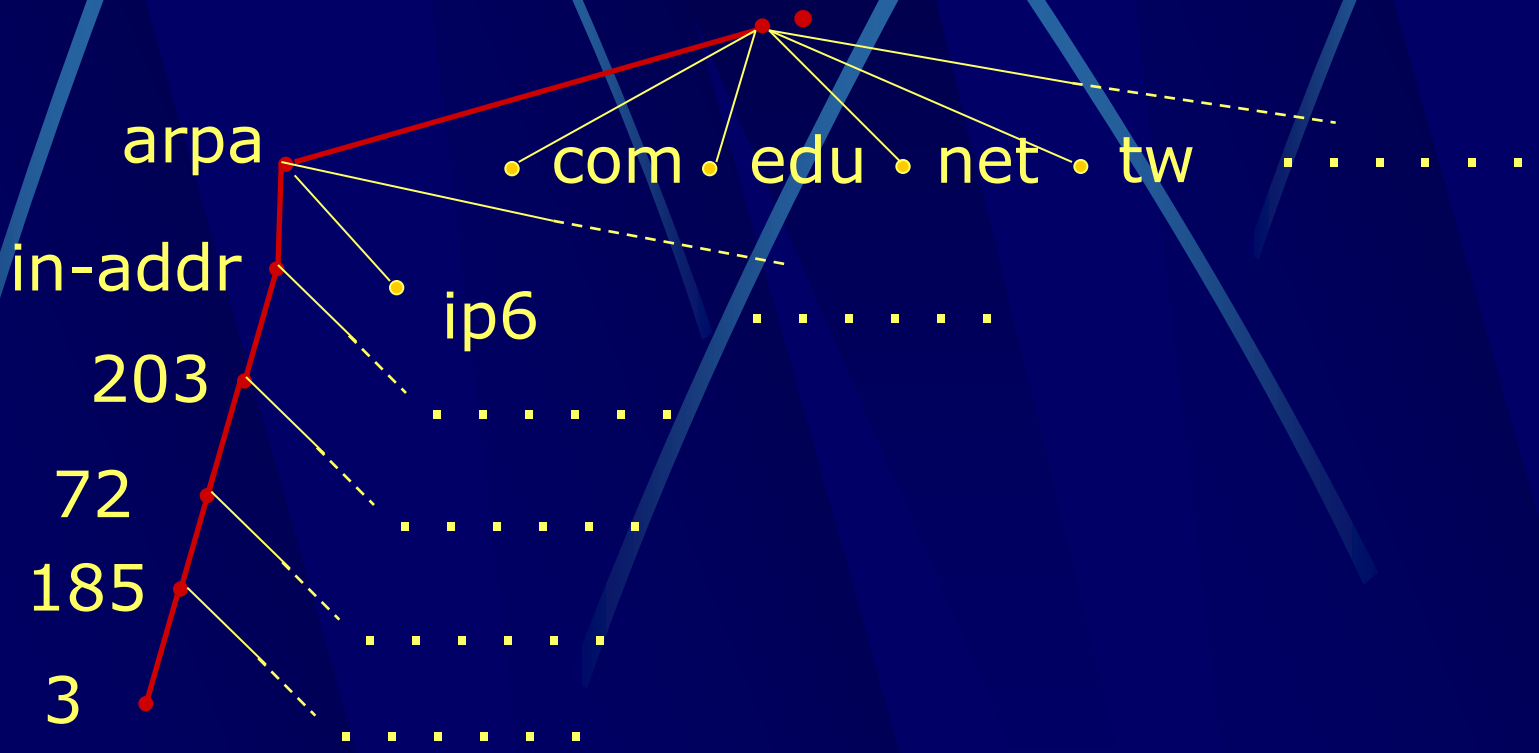
正解之原理

- 正解 tp.edu.tw.



反解之原理

- 反解 3.185.72.203.in-addr.arpa.



Mapping Address to Name

- In-addr.arpa domain are labeled after the numbers in the dotted-octet representation of IP Addresses.
- In-addr.arpa domain可有256個subdomain(對應到IP Address的第一位)
- 每一個subdomain可有256個subdomain(對應到IP Address的第二位)
- 例: 167.249.21.163.in-addr.arpa.
  (dns2.tp.edu.tw)

DNS 的平台

- UNIX
  - 常見為ISC BIND
  - 共約發行三十幾個版本 (4.X~9.X)
  - 最新版本 4.9.9(不再維護)， 8.4.1， 9.2.2
  - 建議使用 9.2.2 版本
  - 穩定，可靠，最多人使用
- Windows
  - 可見於Windows Server 級的版本
  - 簡單設定是其優點
  - GUI 設定
  - 根據 BIND 4.x 修改而來

Configuring Host - resolver

- resolv.conf
  - domain：指出resolver所在的domain name
    - 例: domain ntnu.edu.tw
  - search：指出在查詢domain name時, 附加在domain name後查詢的順序
  - nameserver：查詢的name server(IP)
    - 例: nameserver 140.122.65.9
    - 最多可設三行

Configuring Host - resolver

- resolv.conf
  - sortlist : 從name server查到的IP Address, 如符合所設定之參數, 則跟據sortlist順序排列
    - 例:

```
sortlist  140.122.65.0/255.255.255.0  203.72.188.0/255.255.255.0
```

Type of Name Server

- Master (Primary)
- Slave (Secondary)
- Forwarding
- Cache-Only

Master & Slave Server

- Master -
  - The server for a zone reads the data for the zone from files on its host
- Slave –
  - The server for a zone gets the zone data from another name server that is authoritative for the zone

Forwarding

- If the request records are already in the name server's authorititative data or cached data, the name server answers with the information.
- If the records aren't in tis database, it sends the query to a forwarder.
- If no answer in a short period, it resume normal operation.

Cache Only

- The name servers not authoritative for any zones.

- Name server needs a configuration file –
  - named.conf
- Zone data files –
  - Case-insensitive
  - Resource records must start in the first column of a line
  - Order is not a requirement

Configuration File – named.conf

- BIND (named) 環境之主要設定檔
- 作用
  - 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...

Configuration File – named.conf

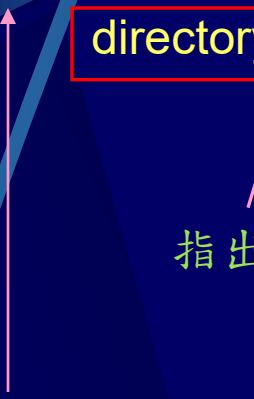
```
options {
        directory  "/var/named";
};
zone "." {
        type hint;
        file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

```
zone “slhs.tp.edu.tw" in {
        type master;
        file "named.hosts";
        allow-query { any; };
        allow-transfer {203.72.185.15;};
};

zone “185.72.203.in-addr.arpa" in {
        type master;
        file "named.rev";
        allow-query { any; };
        allow-transfer {203.72.185.15;};
};
```

Configuration File – named.conf

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



指出data file存放於何處

有關Name Server的選項參數設於option statement中

Configuration File – named.conf

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

- 指出有關root name server的資料存放於何處
- 在BIND 9中, 已內建於程式中,可不設

Configuration File – named.conf

負責的zone是slhs.tp.edu.tw
origin是slhs.tp.edu.tw

角色是primary master

```
zone “slhs.tp.edu.tw" in {
type master;
file "named.hosts";
allow-transfer {203.72.185.15;};
};
```

資料存放在此檔案中

允許203.72.185.15做Zone Transfer

- Forward mapping
- Name-to-Address Mapping

Configuration File – named.conf

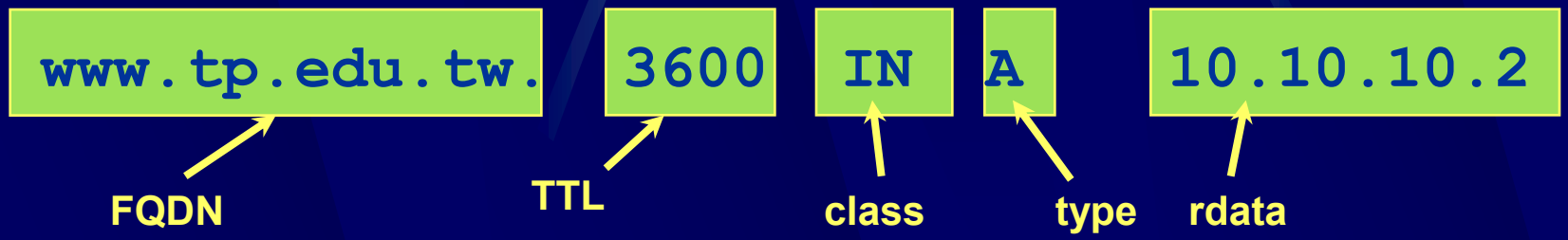
Configuration File – named.conf

設定1.0.0.127之reverse mapping資料

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

資源記錄(Resource Recored)

- 資源記錄(RR， Resource Record)
  - 名稱(FQDN)
  - 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



- SOA record –
  - Authority for this zone
  - Start Of Authority
- NS record –
  - List a name server for this zone
- Other records
  - Data about hosts in this zone
- Comments
  - Start with ; and finish at the end of the line

Other Records

- A
  - Name-to-address mapping
- PTR
  - Address-to-name mapping
- CNAME
  - Canonical name(for alias)
- MX
  - Mail eXchanger

SOA Record -

```
$TTL    86400
@       IN      SOA     dns.slhs.tp.edu.tw.    Sysadm.slhs.tp.edu.tw. (
                        2002022701  ; Serial
                        21600       ; Refresh
                        7200        ; Retry
                        3600000     ; Expire
                        86400 )     ; Negative caching
```

- origin
- 負責的domain name
- 使用與named.conf中所指定的名稱

- IN代表InterNet

SOA Record -

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.  sysadm.slhs.tp.edu.tw. (
                     2002022701  ; Serial
                     21600       ; Refresh
                     7200        ; Retry
                     3600000     ; Expire
                     86400 )     ; Negative caching
```

Primary master name server

此zone管理者的E-Mail Address

將 @ 用 . 取代

SOA Record -

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                        2002022701  ; Serial
                        21600       ; Refresh
                        7200        ; Retry
                        3600000     ; Expire
                        360 )       ; Negative caching
```

- 讓SOA可跨越數行
- ()中的資料大都是給 slave name server使用

SOA Record -

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                     2002022701 ; Serial
                     21600      ; Refresh
                     7200       ; Retry
                     3600000    ; Expire
                     360 )      ; Negative caching
```

- Serial Number
- 每次改變資料,serial number要增加
- Slave server跟據此number來決定是否要傳送master server的資料
- 通常格式為YYYYMMDDNN

SOA Record -

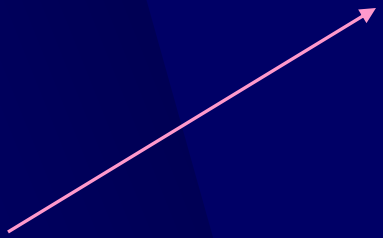
```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                      2002022701  ; Serial
                      21600       ; Refresh
                      7200        ; Retry
                      3600000     ; Expire
                      360 )       ; Negative caching
```

m: 分
h: 小時
d: 天
w: 星期

- 告訴slave server每隔多久要到master server檢查資料是否更新
- 單位為秒
- 亦可直接指定如Hour, 例: 6h, 5h60m

SOA Record -

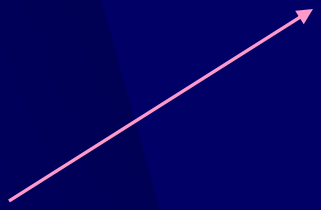
```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                          2002022701  ; Serial
                          21600       ; Refresh
                          7200        ; Retry
                          3600000     ; Expire
                          360 )       ; Negative caching
```



- 如果slave server無法與master server連絡, 則在多久後再試一次

SOA Record -

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                          2002022701  ; Serial
                          21600       ; Refresh
                          7200        ; Retry
                          3600000     ; Expire
                          360 )       ; Negative caching
```



- 如果slave server在這段時間中一直無法與master server連絡，則不再負責此Zone
- expire的設定值應遠大於refresh及retry

SOA Record -

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                          2002022701  ; Serial
                          21600       ; Refresh
                          7200        ; Retry
                          3600000     ; Expire
                          360 )       ; Negative caching
```

- Default TTL
- 告訴querier, name server回應的資料可cache多久

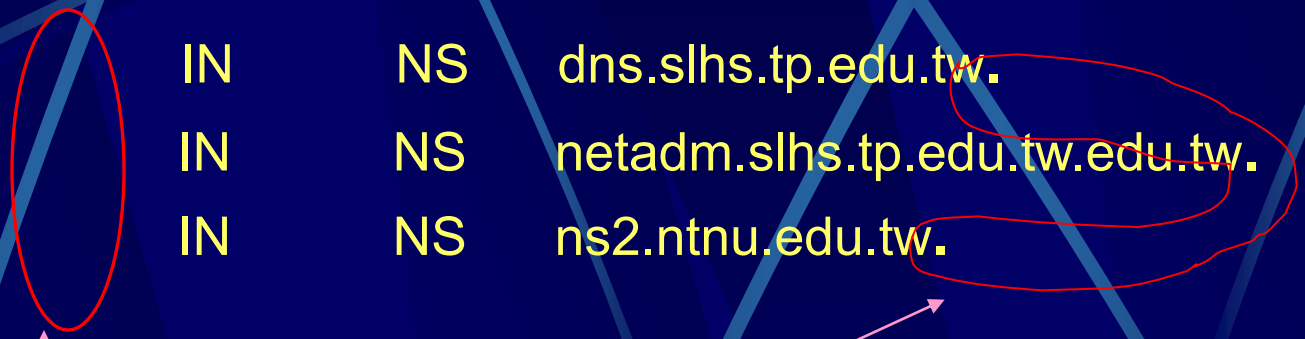
- 對於cache的negative資料要保留多久

SOA Record -

RFC 1537建議

- Refresh 24Hours
- Retry 2 Hours
- Expire 30 Days
- Default TTL 4 Days

NS Record -



```
IN      NS      dns.slhs.tp.edu.tw.
IN      NS      netadm.slhs.tp.edu.tw.edu.tw.
IN      NS      ns2.ntnu.edu.tw.
```

- 每一個負責此zone的name server都要有一行NS Record
- Name server的address須為FQDN, 即最後有一點

如果第一個欄位是空白或Tab, 則延用上一個resource record第一個欄位的name

Address and Alias Record -

dns	IN	A	203.72.185.1
www	IN	A	203.72.185.3
web	IN	CNAME	www
mars	IN	A	203.72.185.22
earth	IN	A	203.72.185.25
proxy	IN	A	203.72.185.11
netadm	IN	A	203.72.185.15
smtp	IN	A	203.72.185.102

- origin為slhs.tp.edu.tw
- 自動在後面加上origin, 例:
  - smtp -> smtp.slhs.tp.edu.tw.

Address and Alias Record -

dns	IN	A	203.72.185.1
www	IN	A	203.72.185.3
web	IN	CNAME	www
mars	IN	A	203.72.185.22
earth	IN	A	203.72.185.25
proxy	IN	A	203.72.185.11
netadm	IN	A	203.72.185.15
smtp	IN	A	203.72.185.102

Address

dns.slhs.tp.edu.tw.之IP Address

Address and Alias Record -

dns	IN	A	203.72.185.1
www	IN	A	203.72.185.3
web	IN	CNAME	www
mars	IN	A	203.72.185.22
earth	IN	A	203.72.185.25
proxy	IN	A	203.72.185.11
netadm	IN	A	203.72.185.15
smtp	IN	A	203.72.185.102

alias

- maps an alias to its canonical name
- 表示www.slhs.tp.edu.tw.有另一個別名叫web.slhs.tp.edu.tw.
- alias名字只能出現在resource record的左手邊,不可在右手邊出現

Address and Alias Record -

www1	IN	A	203.72.185.23
www1	IN	A	203.72.187.100

- Multi-homed Address
- 同一台機器(同一個domain name)有多個IP Address

Address and Alias Record -

www1	IN	A	203.72.185.23
www1	IN	A	203.72.187.100

- Address Sorting
  - DNS lookup return多個IP Address, 如果requestor與name server在同一個network, 則name server會將最近的address放在第一個送會
- Round Robin
  - 如果無Address Sorting功能, 這些Address會輪流排第一

PTR Records -

```
1       IN    PTR  dns.slhs.tp.edu.tw.
3       IN    PTR  www.slhs.tp.edu.tw.
22      IN    PTR  mars.slhs.tp.edu.tw.
25      IN    PTR  earth.slhs.tp.edu.tw.
11      IN    PTR  proxy.slhs.tp.edu.tw.
15      IN    PTR  netadm.slhs.tp.edu.tw.
```

- Address-to-Name Mapping
- Origin是185.72.203.in-addr.arpa.(在named.conf中設定)
- Address should point to only a single name(不可以是canonical name)

Loopback Address

```
$TTL   86400
@      IN   SOA  dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                       2002022701  ; Serial
                       10800       ; Refresh
                       3600        ; Retry
                       3600000     ; Expire
                       1h )        ; Minimun
          IN   NS    dns.slhs.tp.edu.tw.
1         IN   PTR   localhost.
```

- lookback address: 127.0.0.1/24
- 代表自己本身

Root Hints Data

```
.                       3600000   IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000       A     198.41.0.4
.                       3600000       NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000       A     128.9.0.107
.                       3600000       NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000       A     192.33.4.12
                        ⋮
```

- 指出root name server在何處
- 定期到ftp.rs.internic.net更新
- Name Server將root name server list存在記憶體中,叫root hint
- 它不會因TTL到期而被清除

Configuration File – named.conf (Slave Server)

```
options {
        directory  "/var/named";
};
zone "." {
        type hint;
        file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

```
zone “slhs.tp.edu.tw" in {
        type slave;
        file “slhs.zone";
        master {203.72.185.1; };
};

zone “185.72.203.in-addr.arpa" in {
        type slave;
        file “203.72.185.rev";
        master { 203.72.185.1; };
};
```

SubDomain – ccjhs.tp.edu.tw (Subdomain of tp.edu.tw)

origin is tp.edu.tw.

.....

ccjhs IN NS dns1.ccjhs.tp.edu.tw.

```
$ORIGIN     ccjhs.tp.edu.tw.
@       IN  NS  dns1.ccjhs.tp.edu.tw.
        IN  NS  dns2.ccjhs.tp.edu.tw.
dns1    IN  A   163.21.9.200
dns2    IN  A   163.21.9.201
```

dns1.ccjhs.tp.edu.tw.
dns2.ccjhs.tp.edu.tw.

SubDomain – 9.21.163.in-addr.arpa
(Subdomain of 21.163.in-addr.arpa)

origin is 21.163.in-addr.arpa.

.....

```
9        IN    NS    dns1.ccjhs.tp.edu.tw.
         IN    NS    dns2.ccjhs.tp.edu.tw.
```

- 一個zone可設定多個authotitative name server
- Primary Master只有一個
- Slave Master可有多個
- 在NS Records中將所有name server指定
- NS Records並不指出何為Primary, 何為Slave
- Slave Server透過網路從其它name server將data load過來
- 這name server並不限定是Primary Master
- 每個zone的authoritative name server至少要兩個

DNS and E-mail

- MX Records –
  - specify a mail exchanger for a domain name
  - The mail exchanger will process or forward mail for the domain name.
- sendmail在送信前先向DNS詢問destination是否有MX record, 如果沒有, 再向DNS詢問destination之IP Address

MX Record -

- origin是slhs.tp.edu.tw.
- domain name是ms.slhs.tp.edu.tw

- 使用FQDN(最後有一點)

@	IN	MX	0	ms.slhs.tp.edu.tw.
@	IN	MX	10	smtp.slhs.tp.edu.tw.

- preference value
- 避免loop產生
- value越小, priority越高
- 範圍0 ~ 65535

mail exchanger

MX Record -

- origin是slhs.tp.edu.tw.
- domain name是ms.slhs.tp.edu.tw

@	IN	MX	5	smtp.tp.edu.tw.
@	IN	MX	10	smtp.slhs.tp.edu.tw.
@	IN	MX	20	ms.slhs.tp.edu.tw.

- 使用FQDN(最後有一點)
- preference value
- 避免loop產生
- value越小, priority越高
- 範圍0 ~ 65535

mail exchanger

MX Record -

@	IN	MX	5	smtp.tp.edu.tw.
@	IN	MX	10	smtp.slhs.tp.edu.tw.
@	IN	MX	20	ms.slhs.tp.edu.tw.

- mail exchanger必需有address record
- mail excahnger不可為alias name

Security -

- ACL – Access Control List

```
acl  “SLHS-Campus" {
        140.122.64.0/26;
        203.72.185.0/24;
        203.72.187.0/24;
        127.0.0.1;
};
```

Security -

- Restricting Queries

```
options {
        directory "/var/named";
        allow-query {
                SLHS-Campus;
        };
};
```

Security -

- Restricting Queries

```
zone “slhs.tp.edu.tw" in {
        type master;
        file "named.hosts";
        allow-query { any; };
};

zone “185.72.203.in-addr.arpa" in {
        type master;
        file "named.rev";
        allow-query { any; };
};
```

Security -

- Restricting Unauthorized Zone Transfer

```
options {
        allow-transfer {203.72.185.15;140.122.65.221 } ;
        directory "/var/named";
        allow-query {
                NTNU-Campus;
        };
};
```

203.72.185/24 ;

Security -

- Restricting Unauthorized Zone Transfer

```
Zone “slhs.tp.edu.tw” {
    type slave ;
    masters {203.72.185.1; } ;
    file  “ntnu.zone” ;
    allow-transfer { none ; } ;
} ;
```

Forwarding

```
options {
        forwards {140.111.1.2; 168.95.1.1; }
};
```

- If the request records are already in the name server's authorititative data or cached data, the name server answers with the information.
- If the records aren't in tis database, it sends the query to a forwarder.
- If no answer in a short period, it resume normal operation.

Forwarding Only

```
options {
        forwards {140.111.1.2; 168.95.1.1; }
        forward only ;
};
```

- rely complete on its forwarders
- never try to contact other name server, even the forwarders don’t give it answer

Caching-Only Server

name servers not authorirative for any zones.

```
options {
    directory  “/var/named” ;
} ;

zone  “0.0.127.in-addr.arpa” {
    type  master ;
    file  “named.local” ;
} ;
```

```
zone  “.” {
    type  hint ;
    file  “named.ca” ;
} ;
```

Bogus Name Server

```
options {
        server 168.235.1.1 {
                bogus yes ;
        } ;
};
```

- configure name server not to ask questions of this server.

Blackhole Name Server

```
options {
        blackhole  {
            10/8 ;
            192.168/16 ;
        } ;
};
```

- configure name server not query name servers on the list and not respond queries from these servers.

Dynamic Update

```
zone "ntnu.edu.tw" in {
        type master;
        file "named.hosts";
        allow-update  { 203.72.185.100 ; };
};
```

Dynamic Update

```
zone “slhs.tp.edu.tw" in {
        type slave;
        file “slhs.zone";
        allow-update  { 203.72.185/24 ; };
};
```

Only updates from IP address that match the address match list will be forwarded.

負載平衡功能 (Round Robin)

www	**IN**	**A**	**203.72.185.3**
www	**IN**	**A**	**203.72.185.4**
pc1	**IN**	**A**	**203.72.185.100**
pc2	**IN**	**A**	**203.72.185.200**

- 如上資料，一個 FQDN 有兩個以上之 IP 位址是允許的
- 回答的答案基本上是亂數決定的，不過在 BIND 9.X 中是以有些回答的依據設定 (rrset)
- DNS 僅做名稱之負載平衡，如 www/mail 或他類型的服務之負載平衡要取決其他技術(ex:Level 4 switch)

Subnetting on a Non-Octet Boundary

- Forward Mapping不會有問題
- Reverse Mapping要如何做?
  - 統一管理
    - 由某一單位統一管理某一IP Subnet之Reverse Mapping
    - 所有變動均須通知該管理單位更新PTR Record
  - 授權各單位自行管理維護
    - Parent Name Server須定義那些要授權

Subnetting on a Non-Octet Boundary

如果將 163.21.100/24 切割為16個 subnet (即 /28)或更小，分配給 16 個學校，DNS 反解應如何設呢？

Subnetting on a Non-Octet Boundary

- 授權各單位自行管理維護
- 163.21.100.1-15授權由dns.xxx.tp.edu.tw管理

```
1.100.21.163.in-addr.arpa.      IN    NS    dns.xxx.tp.edu.tw.
2.100.21.163.in-addr.arpa.      IN    NS    dns.xxx.tp.edu.tw.
.....

15.100.21.163.in-addr.arpa.     IN    NS    dns.xxx.tp.edu.tw.
```

```
$GENERATE  1-15   $.100.21.163.in-addr.arpa.    IN   NS   dns.xxx.tp.edu.tw.
```

```
$ORIGIN 100.21.163.in-addr.arpa.
; 將 16 個子網授權出去： 第一個部門
sch1-16          IN      NS      dns1.xxx.tp.edu.tw.
sch1-16          IN      NS      dns2.xxx.tp.edu.tw.
;第二個部門
sch2-16          IN      NS      dns1.yyy.tp.edu.tw.
sch2-16          IN      NS      dns2.yyy.tp.edu.tw.
;依此類推 16 個部門，
;以 $GENERATE 的方式，建立 CNAME ，將查詢轉往子網：
$GENERATE  0-15                  $       CNAME       $.sch1-16
$GENERATE  16-31                 $       CNAME       $.sch2-16
;依此類推 16個部門
```

- 有人查詢 163.21.100.1 之反解時，會查到其 CNAME 至 1.sch1-16.100.21.163.in-addr.arpa.
- 此時 sch1 學校的對等反解域名應定義為
  - ***zone “sch1-16.100.21.163.in-addr.arpa”***

```
#/etc/named.conf
zone “sch1-100.21.163.in-addr.arpa” {
    type master;
    file “sch1-100.21.163.rev”;
};
```

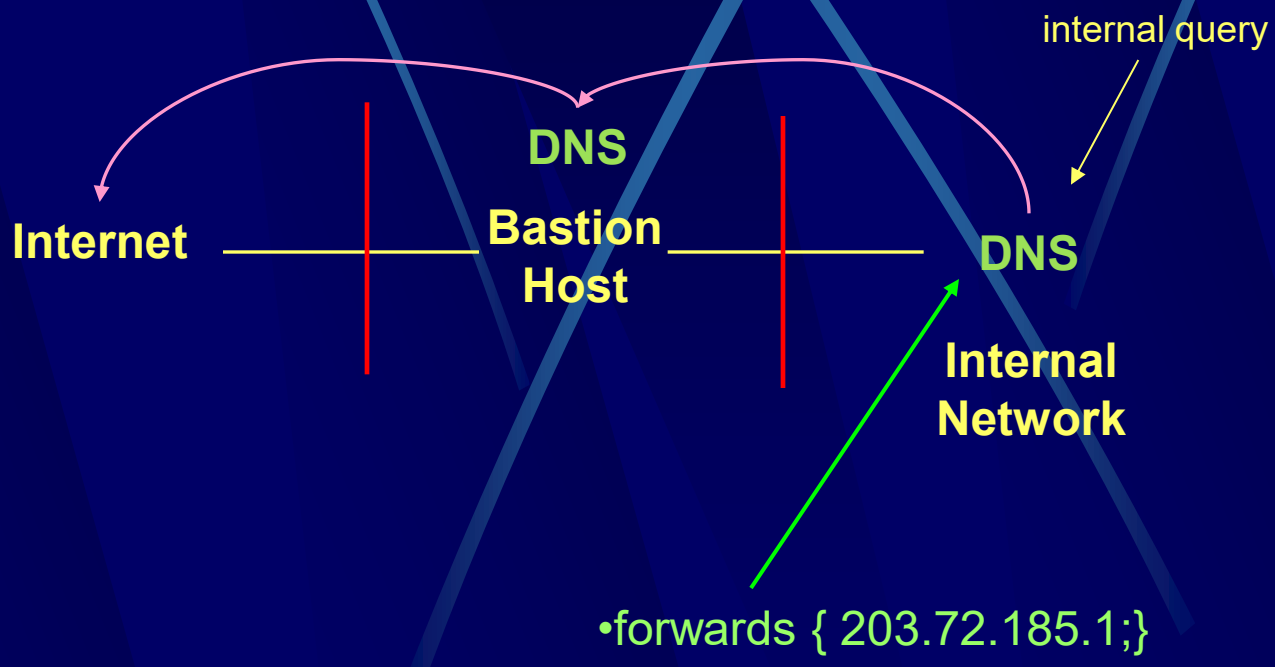
```
;file sch1-100.21.163.rev
;SOA/NS 訊息略
$ORIGIN sch1-100.21.163.in-addr.arpa.
1          IN        PTR      dns1.xxx.tp.edu.tw.
2          IN        PTR      dns2.xxx.tp.edu.tw.
$GENERATE 3-15        $         PTR                pc$.xxx.tp.edu.tw.
```

DNS and Firewalls

- Two major families of firewall software
  - packet filters
    - operate at transport and network level
    - transport protocol(TCP/UPD)
    - IP Address
    - network port
  - application gateways
    - operate at application protocol level

DNS and Firewalls -

Using forwarders



DNS and Firewalls -

```
options {
        .....
        forwards {203.72.185.1;} ;
} ;
zone  “private.ntnu.edu.tw” {
        type  slave;
        masters {192.168.1.1; } ;
        file  “private.zone” ;
        forwards { } ;
} ;
```

DNS and Firewalls -

```
acl  “internal” {
      192.168/24 ;
}
View  “internal”  {
     match-clients { “internal”; } ;
     recursion yes ;
     zone  “slhs.tp.edu.tw” {
        type  master ;
       file “private.zone” ;
     }
    …….
}
```

DNS and Firewalls -

```
View  “external”  {
    match-clients { any; } ;
    recursion no ;
    zone  “slhs.tp.edu.tw” {
       type  master ;
      file “private_ext.zone” ;
    }
    ……
}
```

常見之錯誤

- 資料更新後沒有將serial number增加

```
@     IN     SOA    dns.slhs.tp.edu.tw.   sysadm.slhs.tp.edu.tw. (
                     2002022701 ; Serial
```

- primary master server資料更新後沒有reload系統

  Kill –HUP <PID>

常見之錯誤

- slave server無法從primary server load資料
  - allow-transfer沒設(master端)

```
allow-transfer {203.72.185.15;140.122.65.221; } ;
```

  - master name server之IP Address錯誤

```
master { 203.72.185.1; };
```

  - 網路問題
  - Master之zone data file有問題
    - 例: syntax error

常見之錯誤

- 增加(修改)forward mapping資料後，沒有加入(修改)對應之PTR Record

news	IN	A	203.72.185.101
101	IN	PTR	news.slhs.tp.edu.tw.

常見之錯誤

- 在zone data file中，忘記加上tailling dot.

```
        IN    NS    dns.slhs.tp.edu.tw.
101     IN    PTR   news.slhs.tp.edu.tw.
@       IN    MX    5    smtp.slhs.tp.edu.tw.
```

常見之錯誤

- Missing Subdomain Delegation
  - 沒有跟Parent Name Server註冊
- local domain name not set
  - resolv.conf中未設domain

```
domain      slhs.tp.edu.tw
nameserver  203.72.185.1
```

Incorrect Subdomain Delegation (lame server)

```
$TTL    86400
@       IN      SOA     dns.slhs.tp.edu.tw.    sysadm.slhs.tp.edu.tw. (
                        2002022701  ; Serial
                        21600       ; Refresh
                        7200        ; Retry
                        3600000     ; Expire
                        360 )       ; Negative caching
        IN      NS      dns.slhs.tp.edu.tw.
        IN      NS      netadm.slhs.tp.edu.tw.
        IN      NS      dns.hinet.net.
```

TTL not set

```
$TTL    86400
@       IN      SOA  dns.slhs.tp.edu.tw.    sysadm.slhs.tp.edu.tw. (
                          2002022701  ; Serial
                          21600       ; Refresh
                          7200        ; Retry
                          3600000     ; Expire
                          360 )       ; Negative caching
              IN    NS     dns.slhs.tp.edu.tw.
              IN    NS     netadm.slhs.tp.edu.tw.
              IN    NS     ns2.ntnu.edu.tw.
```

常見之錯誤

- zone transfer fails because of proprietary WINS record
  - “Setting only affect local server” filter out the WINS record for that zone.

@ IN WINS &IP Address of WINS Server

Debug Tool

- nslookup
- dig

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...

以nslookup追蹤(1)

```
[root@pc071 named]# nslookup
Default Server:  dns1.tp.edu.tw
Address:  163.21.249.166

> set q=soa
> tp.edu.tw.
Server: dns1.tp.edu.tw
Address: 163.21.249.166

tp.edu.tw
        origin = tp.edutw
        mail addr = netadm.tp.edu.tw
        serial = 2003111301
        refresh = 86400 (1D)
        retry   = 3600 (1H)
        expire  = 604800 (1W)
        minimum = 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

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

當您查詢 SOA 訊息時，一併
會列出其 NS 資訊，及 NS 的 A 記錄，若您見到的不是這樣的訊息與對應關係，代表您的 DNS 設定有問題

- 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:  dns1.tp.edu.tw
Address:  163.21.249.166

> 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  dns1.tp.edu.tw.
>ls –d  tp.edu.tw.
;以下會列出 tp.edu.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.tp.edu.tw.
Server:  dns.tp.edu.tw
Address:  163.21.249.166

Name:    www.tp.edu.tw
Addresses:  163.21.249.178

>www.msn.com.
Server:  dns.tp.edu.tw
Address:  163.21.249.166

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.msn.com.資訊，列出多IP，即是此記錄做 Round Robin，再查一次可能是相同順序，亦可能某個IP會排到前面，如果您在看此網站，有時可能會連到 207.68.171.247，但有時又會連到207.68.171.244，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

Dig(1) -

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
```

Dig(2) -

```
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.
```

Dig(3) -

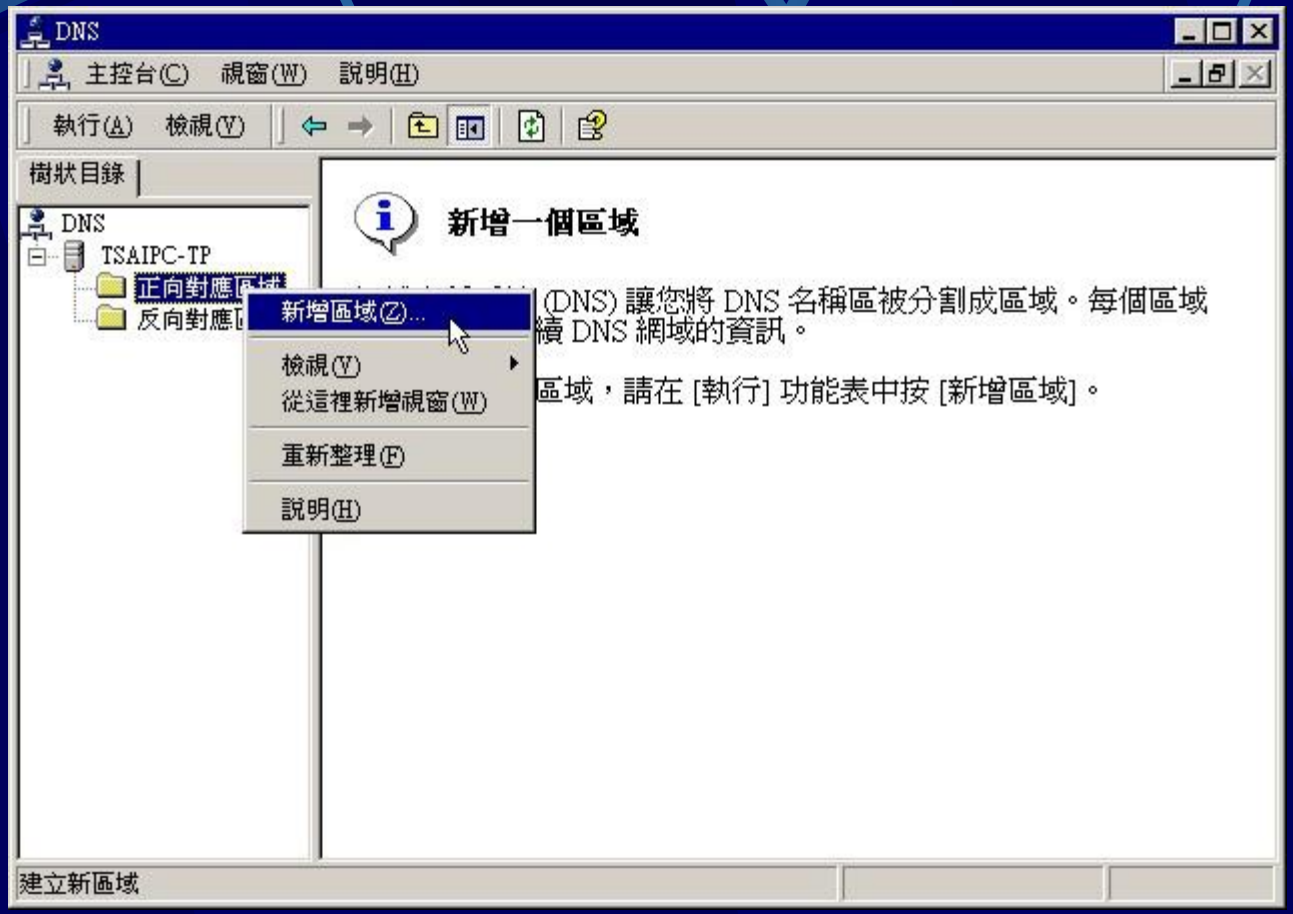
```
root@dns ~ > dig  ibm.com  ns

; <<>> 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.
```

Win2000 DNS – Create New Zone



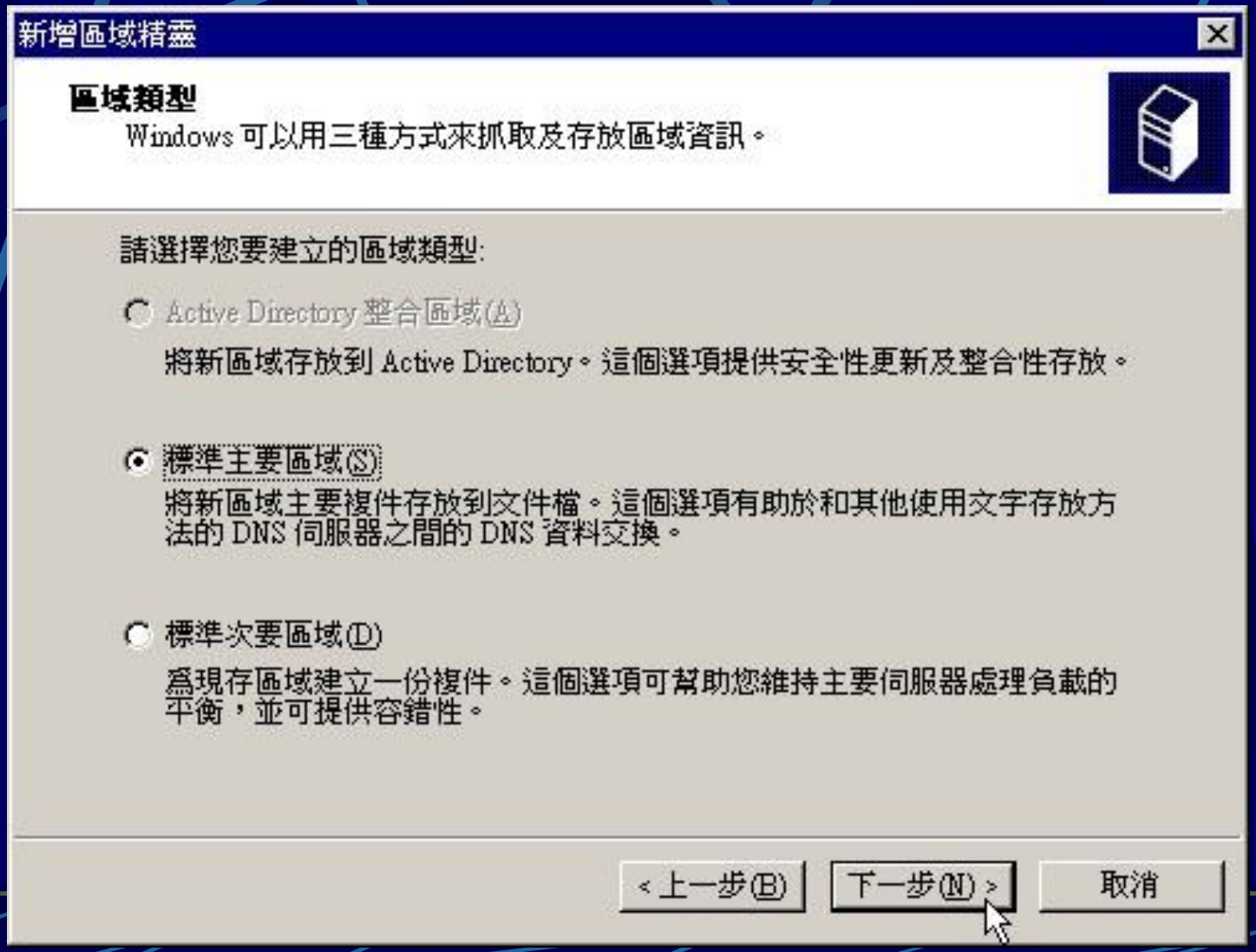
Win2000 DNS – Create New Zone

Win2000 DNS – Create New Zone

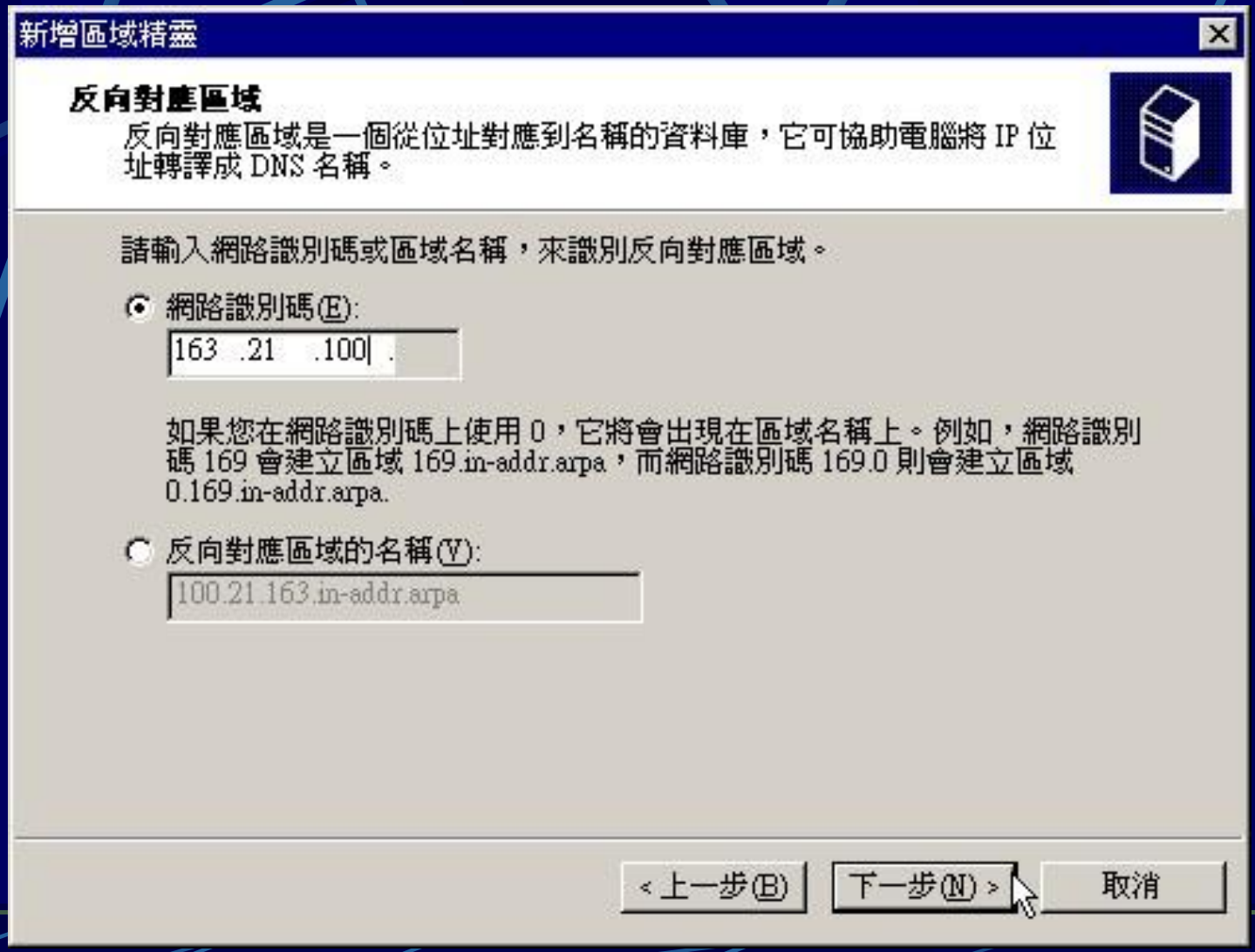
Win2000 DNS – Create New Zone

Win2000 DNS – Create New Reverse-Mapping Zone

Win2000 DNS – Create New Reverse-Mapping Zone

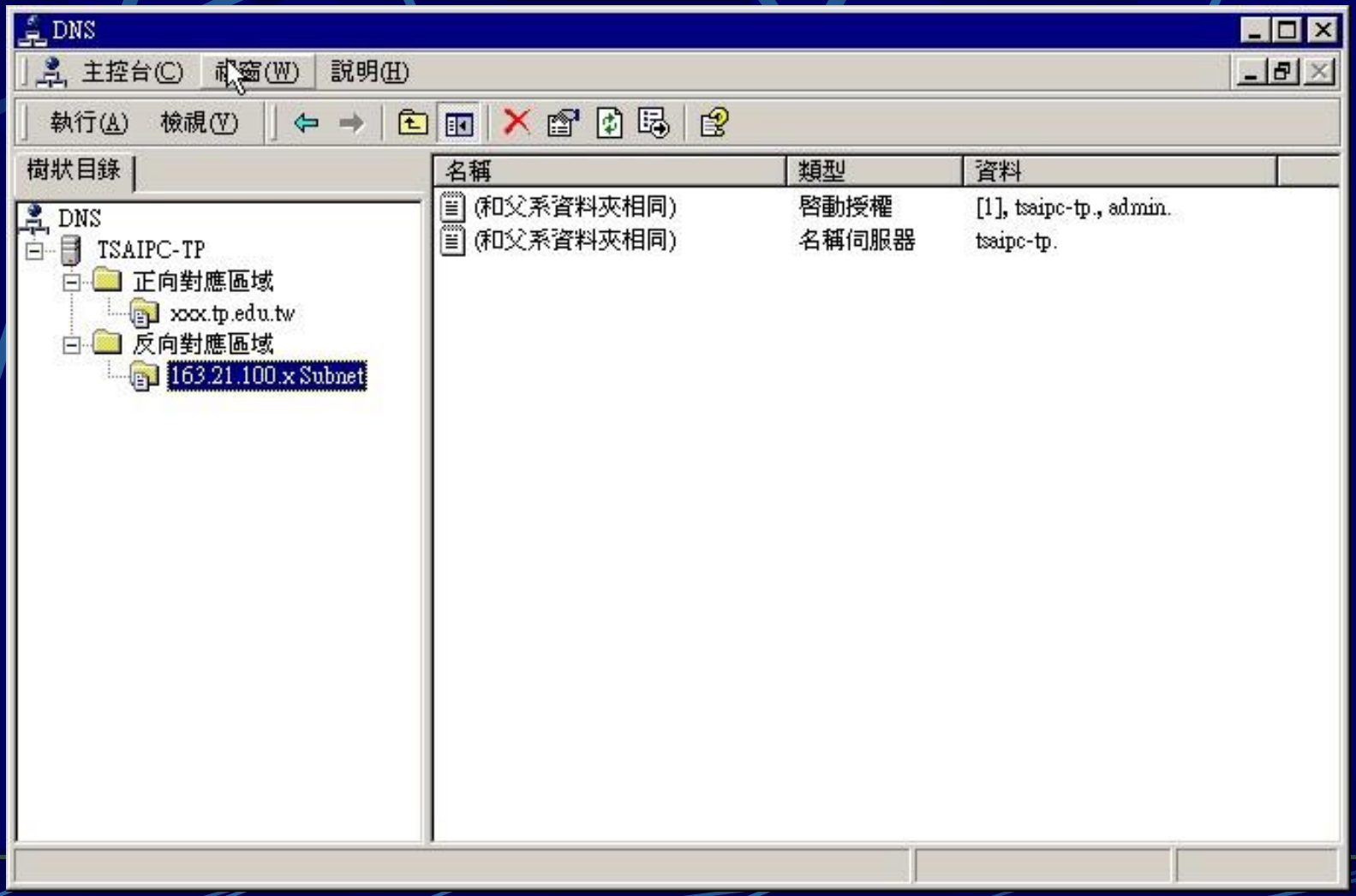


Win2000 DNS – Create New Reverse-Mapping Zone

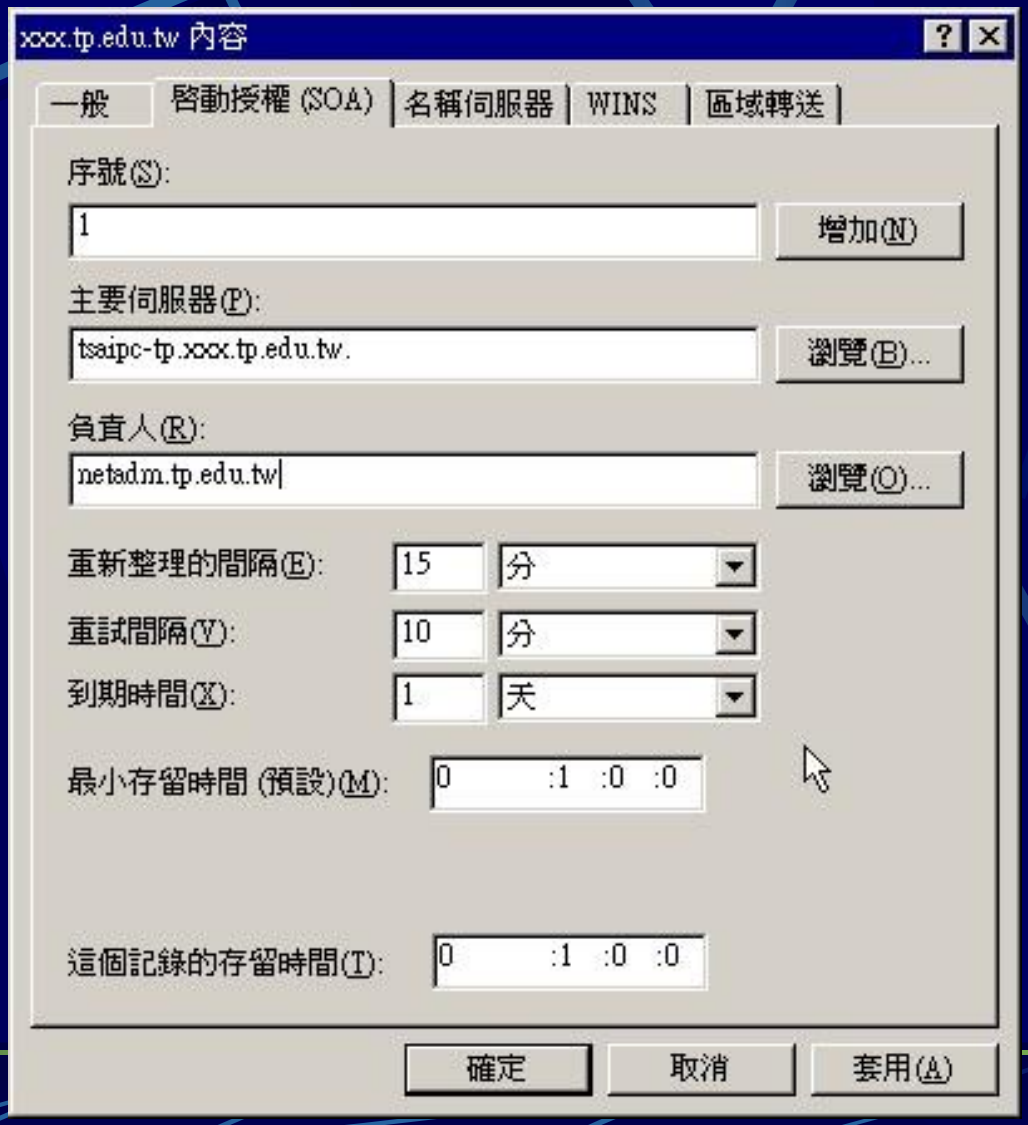


Win2000 DNS – Create New Reverse-Mapping Zone

Win2000 DNS – Create New Reverse-Mapping Zone



Win2000 DNS – SOA Record

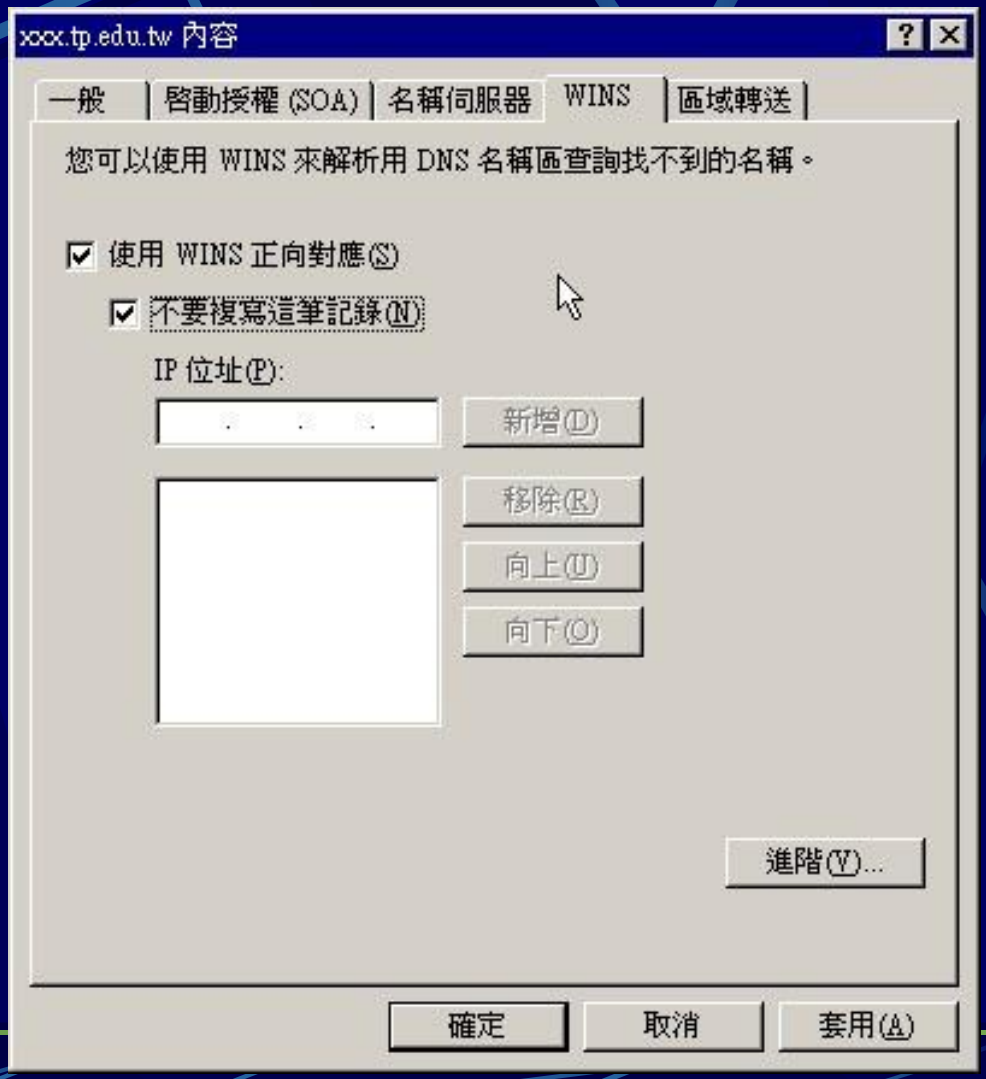


Win2000 DNS – Add NS Record

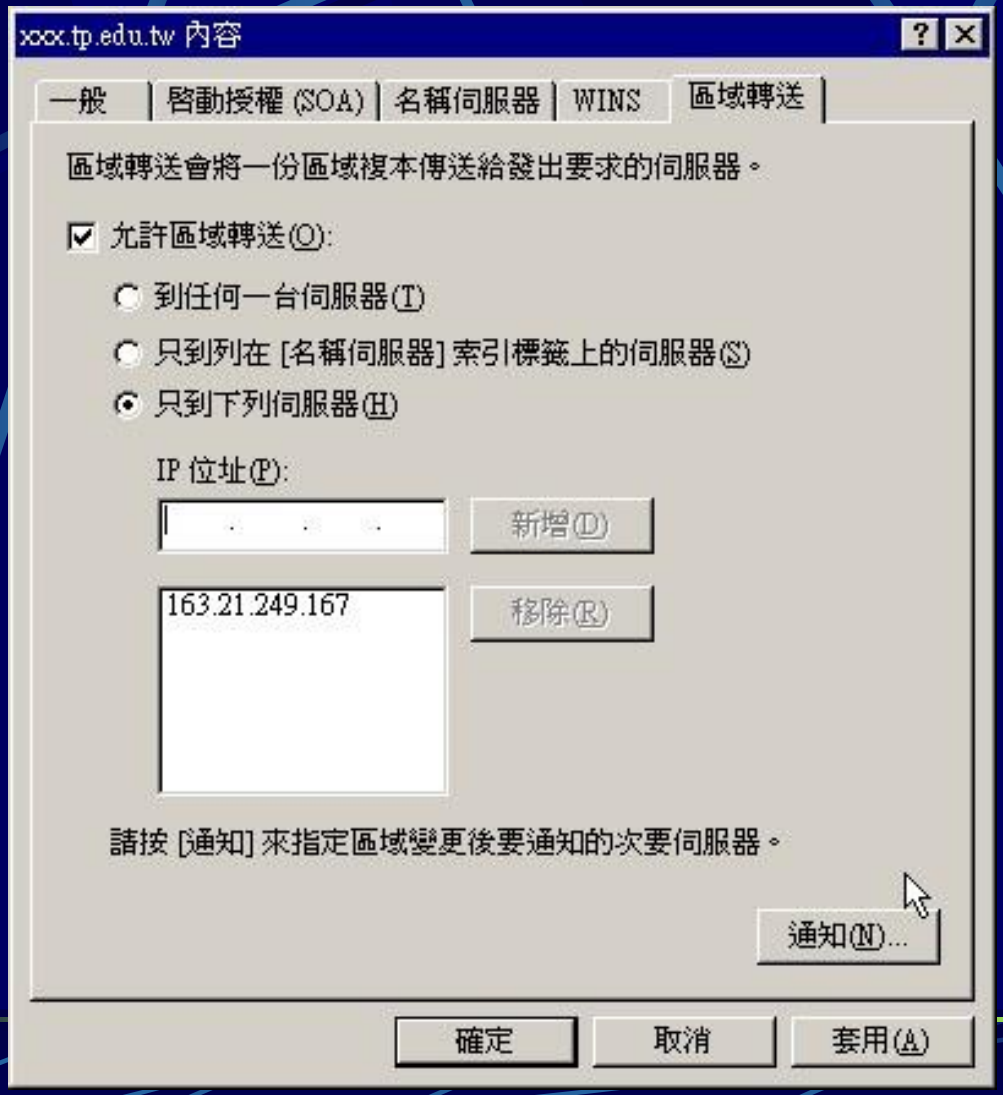
輸入負責此Domain之Name Server
Master及Slave均需輸入

Win2000 DNS – Add NS Record

Win2000 DNS – WINS



Win2000 DNS – Zone Transfer

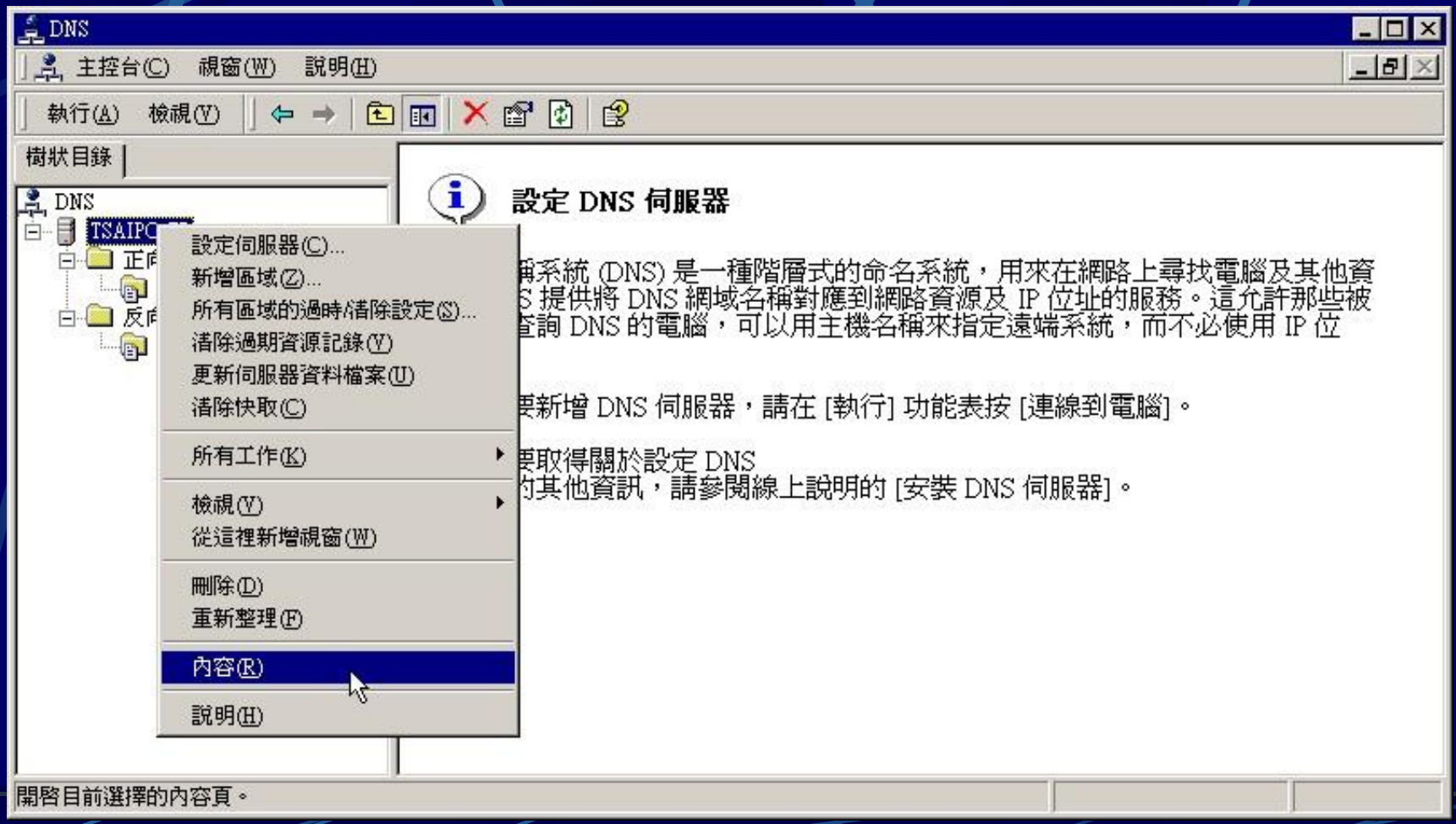


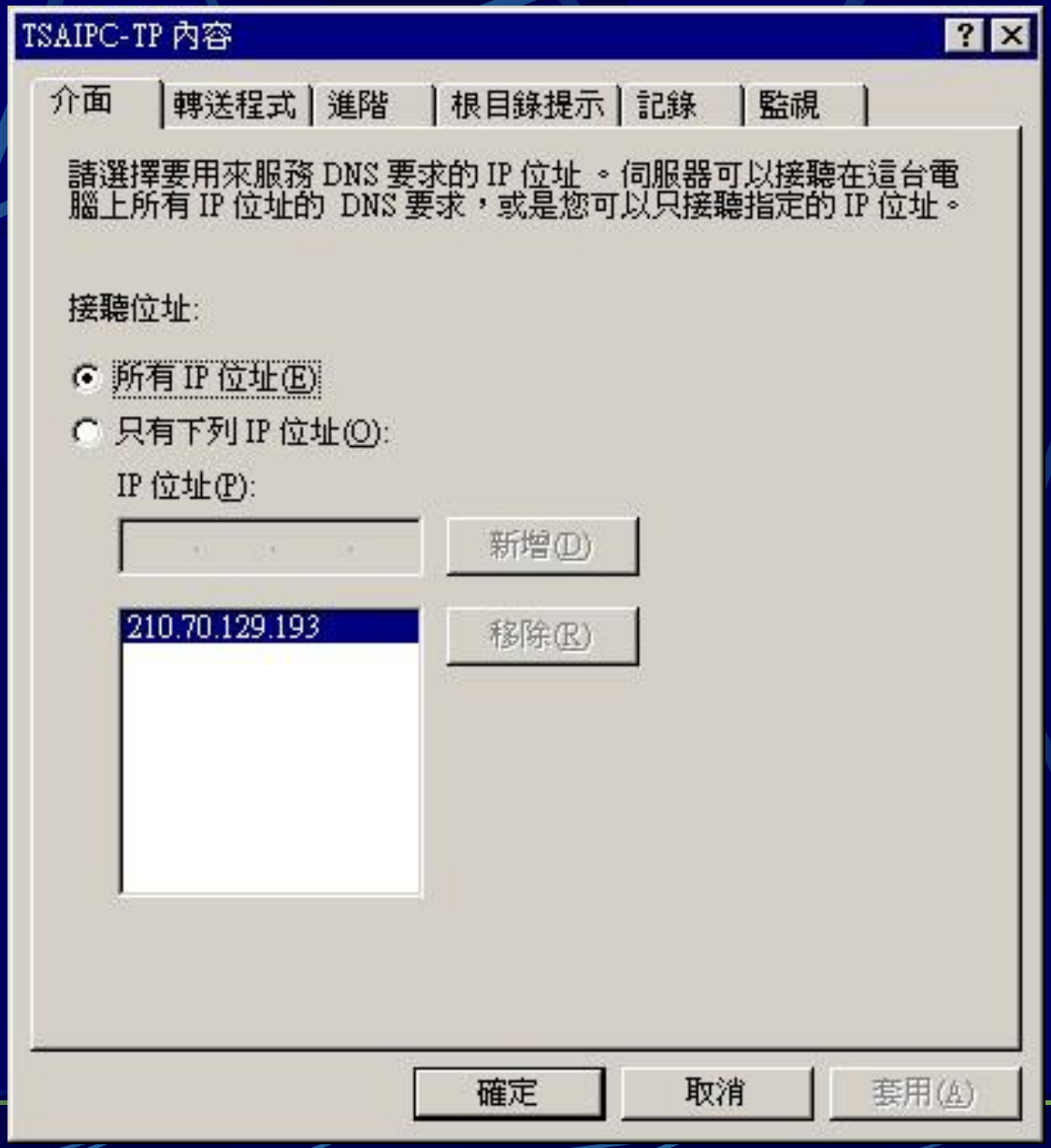
允許誰可以跟你做Zone Transfer

Win2000 DNS – NOTIFY

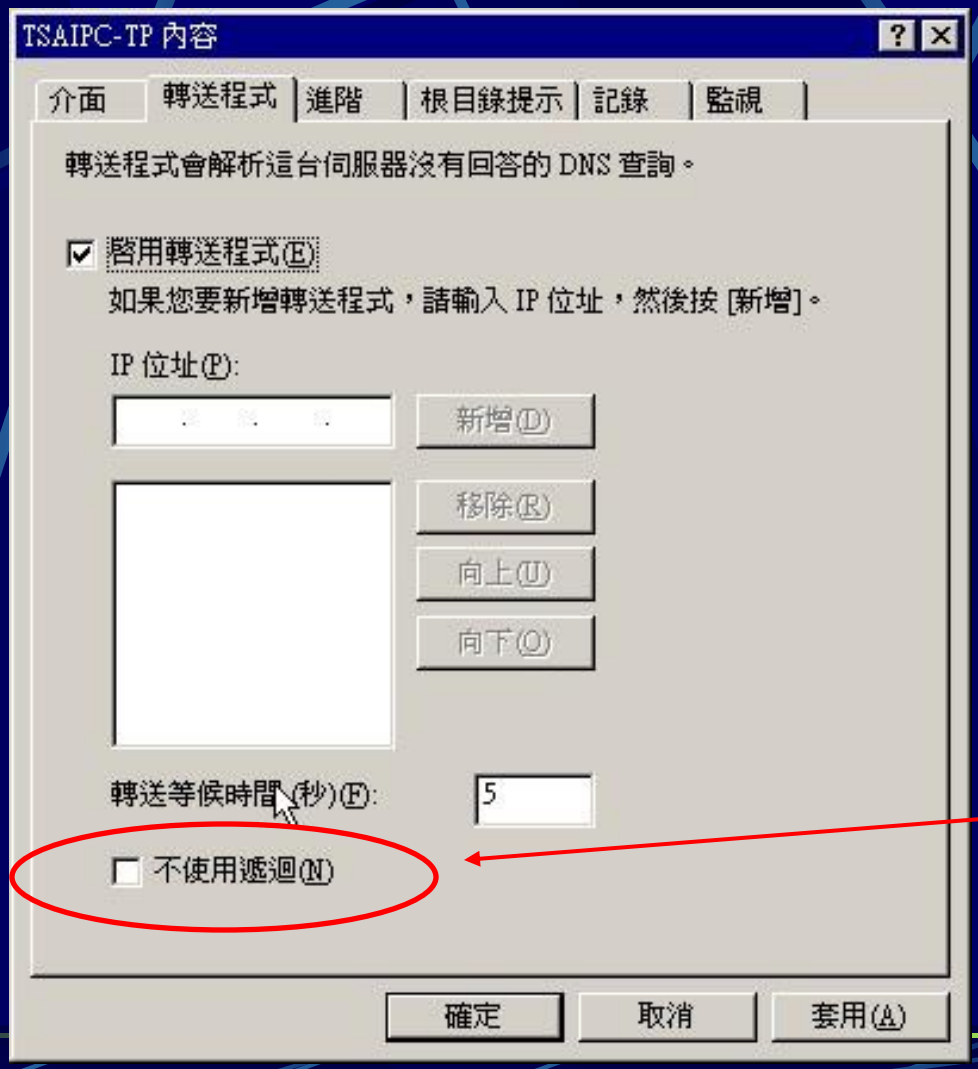
當Zone Data變更時要跟那些Name Server送出Notify訊息

Win2000 DNS


DNS
主控台(C)
視窗(W)
說明(H)
執行(A)
檢視(V)
樹狀目錄
DNS
TSAIPC
正向
反向
設定伺服器(C)...
新增區域(Z)...
所有區域的過時/清除設定(S)...
清除過期資源記錄(V)
更新伺服器資料檔案(U)
清除快取(C)
所有工作(K)
檢視(V)
從這裡新增視窗(W)
刪除(D)
重新整理(F)
內容(R)
說明(H)
設定 DNS 伺服器
系統 (DNS) 是一種階層式的命名系統，用來在網路上尋找電腦及其他資
S 提供將 DNS 網域名稱對應到網路資源及 IP 位址的服務。這允許那些被
查詢 DNS 的電腦，可以用主機名稱來指定遠端系統，而不必使用 IP 位
要新增 DNS 伺服器，請在 [執行] 功能表按 [連線到電腦]。
要取得關於設定 DNS
的其他資訊，請參閱線上說明的 [安裝 DNS 伺服器]。
開啓目前選擇的內容頁。

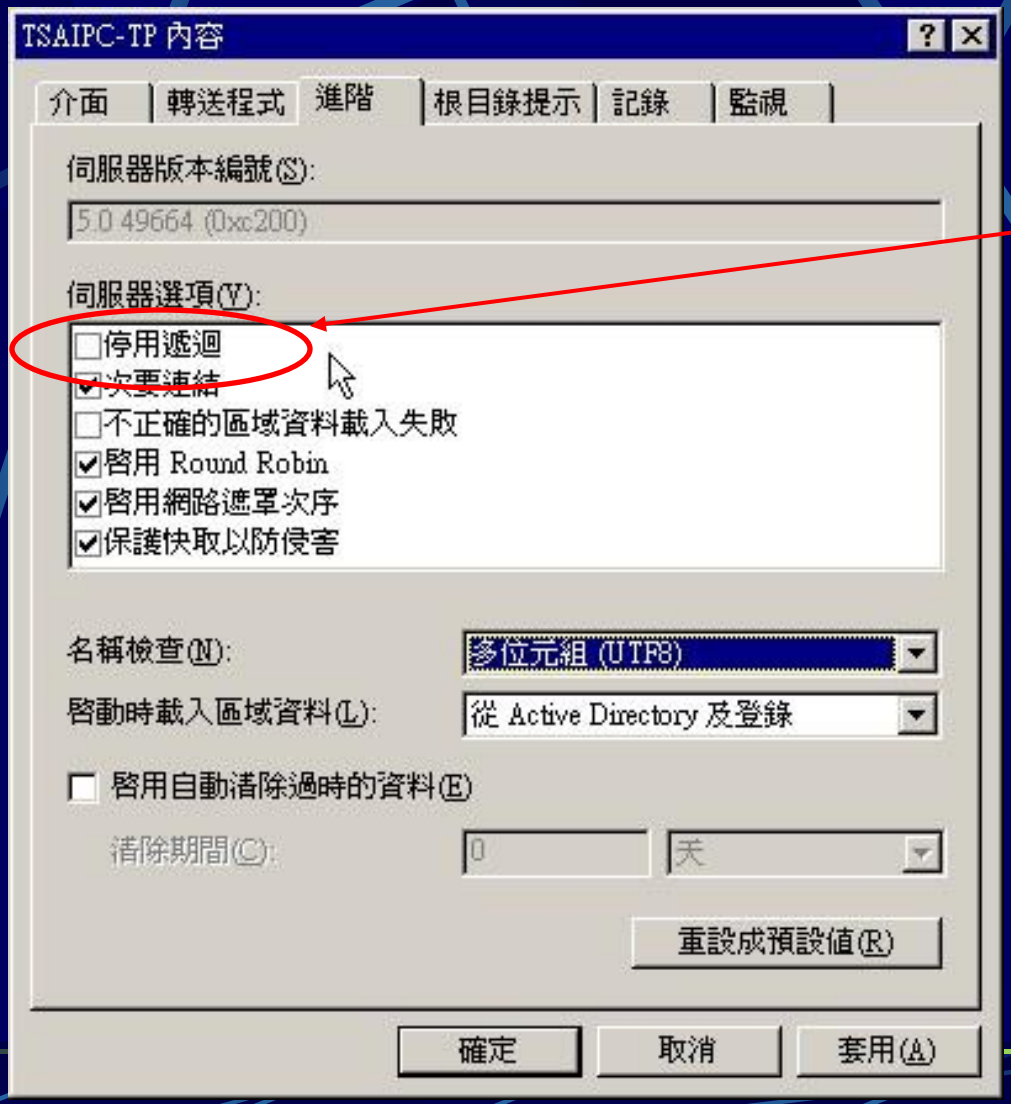

TSAIPC-TP 內容
介面
轉送程式
進階
根目錄提示
記錄
監視
請選擇要用來服務 DNS 要求的 IP 位址。伺服器可以接聽在這台電腦上所有 IP 位址的 DNS 要求，或是您可以只接聽指定的 IP 位址。
接聽位址:
所有 IP 位址(E)
只有下列 IP 位址(O):
IP 位址(P):
新增(D)
210.70.129.193
移除(R)
確定
取消
套用(A)

Win2000 DNS – Forwarder



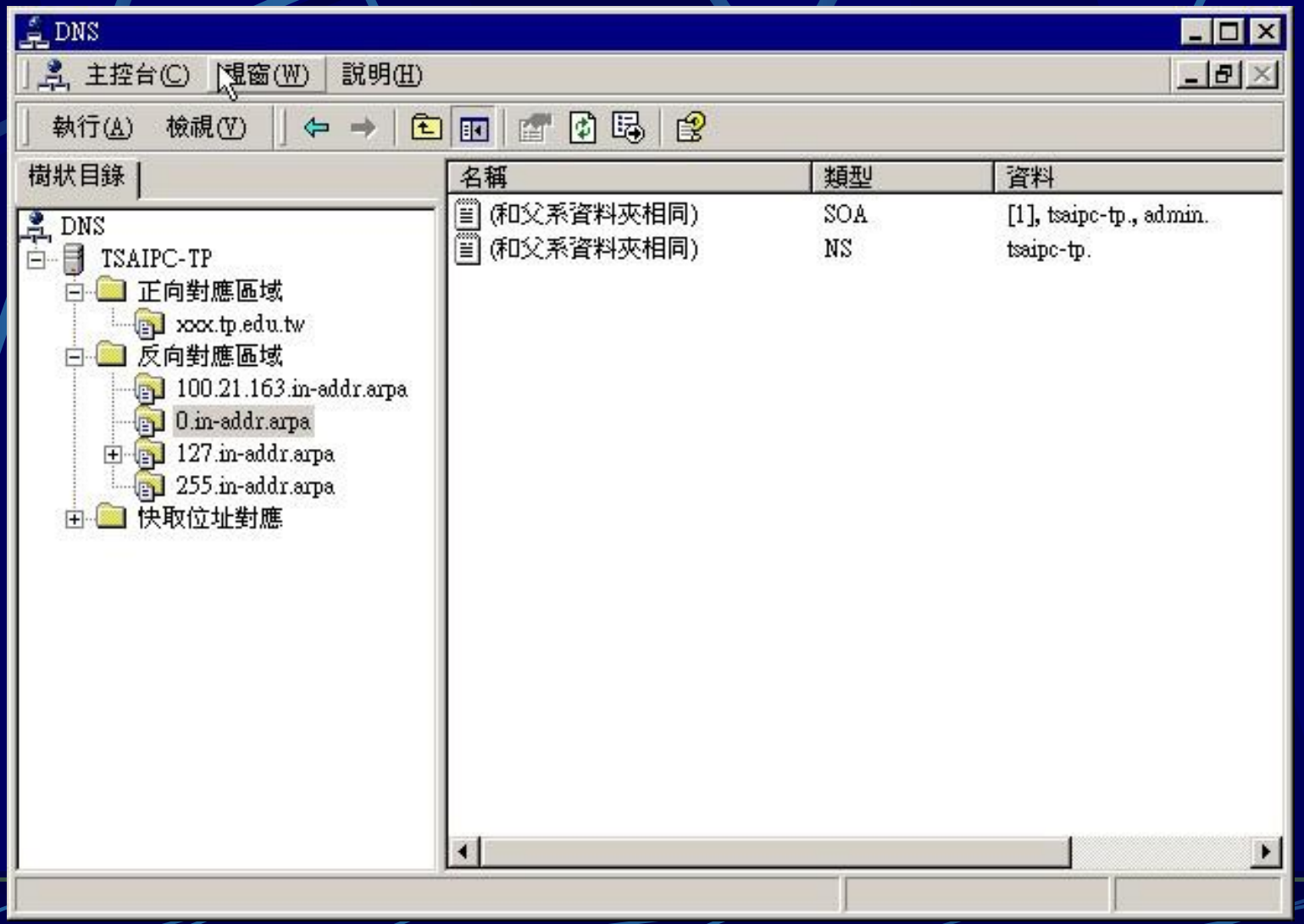
Forward Only

Win2000 DNS

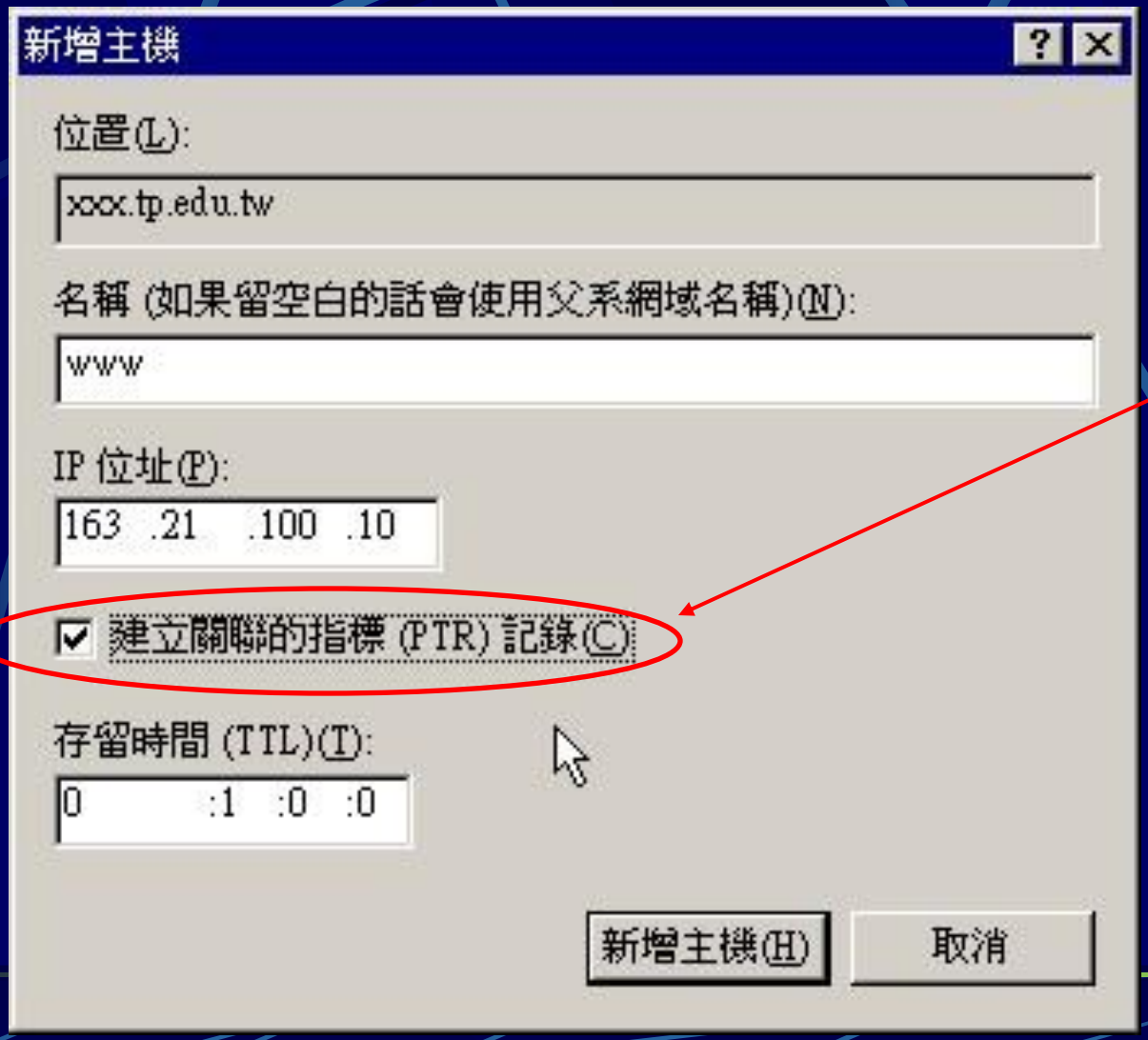


Do Not Answer Recursive Query

Win2000 DNS – Advance Mode

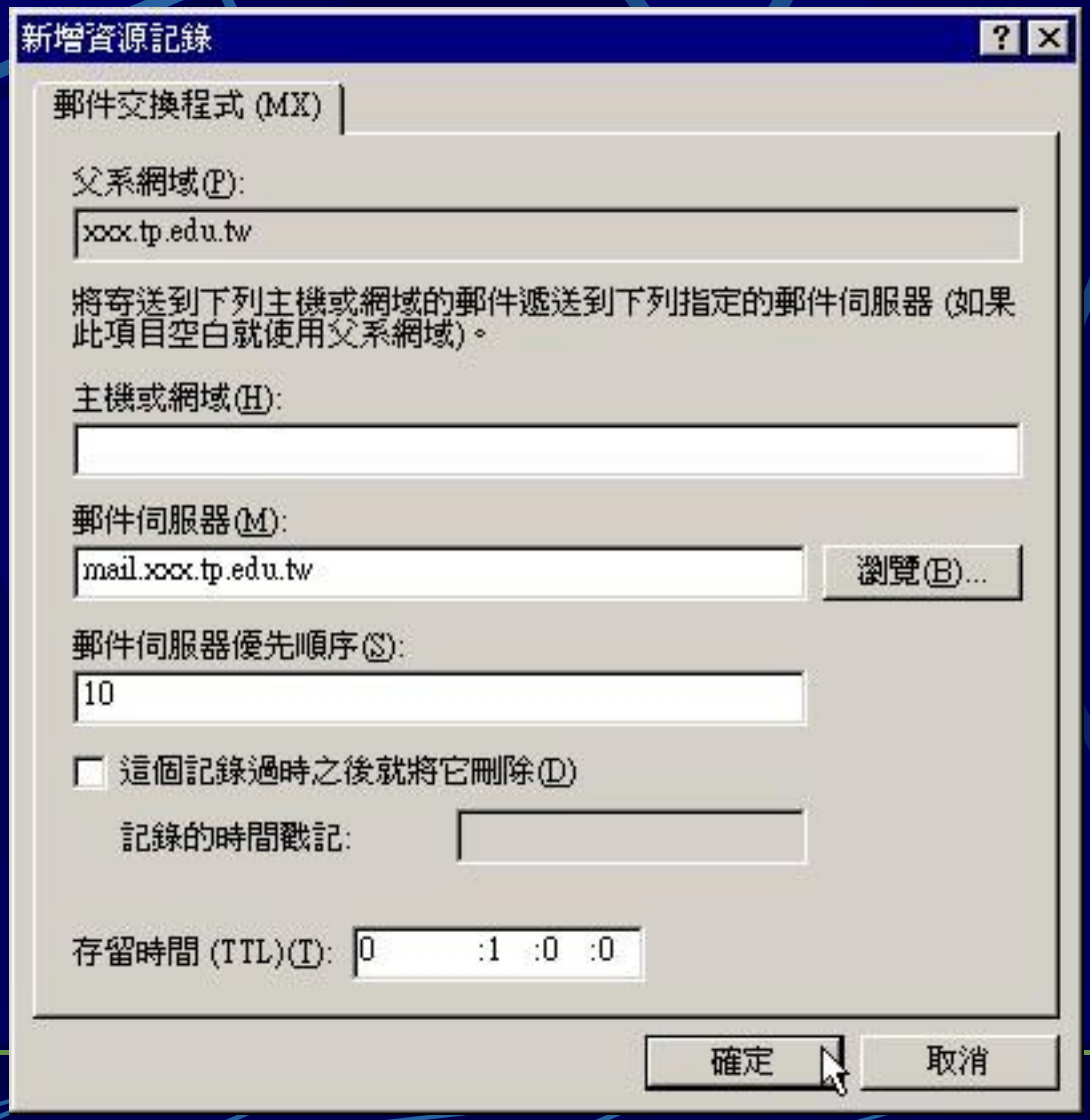


Win2000 DNS – Add A Record



一併建立PTR Record

Win2000 DNS – Add MX Record



DNS 不安全之後果 (1)

- 為何會不安全
  - 被入侵: 可能從別的服務程式或直接從 DNS 入侵
  - 被欺騙: 被造假的 DNS 訊息欺騙
  - 若使用 BIND 建議您昇級至 9.2.2 最新版
- 可能的後果
  - 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

    原來的 www 位於 211.72.211.80，但被改到 1.2.3.4，而其又 mirror 您的網頁，此時很容易套出您使用者的身份與密碼，而又不易被察覺(因為使用者輸入的是 www.xxx.com.tw)(即一般俗稱 man in middle 手法)

DNS 不安全之後果 (2)

- 可能的後果
  - **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。如您的防火牆信任 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 中漆加他機器為 any.com.tw 網域機器的資訊
  - **系統權限**

    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 DNS 權限

名 詞 解 釋

AXFR	同 zone transfer
CIDR	Classless Inter-Domain Routing, RFC1519
DN	網域名稱(Domain Name)
NS	名稱伺服器(Name Server)
RR	資源記錄 (Resource Record)
TTL	time to live ， 存活時間
delegation	委任/授權
negative answers	負面答案，查不到的狀況
Lame Server	不良的委任記錄
zone	轄區
zone transfer	轄區傳送

DNS相關資源

- RFC 1034: domain names - concepts and facilities
- RFC 1035:domain names - implementation and specification
- RFC 1886:DNS Extensions to support IP version 6
- RFC 1912 Common DNS Operational and Configuration Errors
- RFC 2065:Domain Name System Security Extensions
- RFC 2136:Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 3490 IDNA: Internationalizing Domain Names in Applications
- RFC 3491 Nameprep: A Stringprep Profile for Internationalized Domain Names
- RFC 3492 Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications
- BIND 官方網站 http://www.isc.org
- http://www.dns.net/dnsrd/
- http://www.menandmice.com/
- http://dns-learning.twnic.net.tw/
- http://ns.nctu.edu.tw/ http://dnsrd.nctu.edu.tw/

參　考　資　料

- DNS and BIND 4th, O'Reilly
- The Concise Guide to DNS and BIND, QUE
- DNS on Wondows 2000 2nd, O'Reilly
- DNS & BIND Cookbook, O'Reilly