

Windows 及 Linux DNS Server 建置實務 (含 IPv4 與 IPv6)

課程時間：106 年 10 月 6 日

主辦單位：教育部資訊及科技教育司

承辦單位：臺中區域網路中心(國立中興大學)

『Windows 及 Linux DNS Server 建置』課程大綱

時 間	課程內容
08:30 – 09:00	報到
09:00 – 10:20	➤ DNS 基礎介紹P1 <ul style="list-style-type: none"> ● DNS 基礎概念 ● DNS Server 角色介紹 ● DNS 正向查詢解析與反向查詢解析介紹
10:20 – 10:40	中場休息
10:40 – 12:00	➤ Windows Server 2012 升級 IPv6 實作教學.....P13 <ul style="list-style-type: none"> ● Server 設定 IPv6 位址與連線 ● DNS Server 升級 IPv6 ● Web Server 升級 IPv6
12:00 – 13:00	中午用餐
13:00 – 14:20	➤ Windows Server 2012 升級 IPv6.....P37 <ul style="list-style-type: none"> ● 新增委派 DNS
14:20 – 14:40	中場休息
14:40 – 16:00	➤ Linux Server 升級至 IPv6P45 <ul style="list-style-type: none"> ● Linux 的 IPv6 設定 <ul style="list-style-type: none"> ✧ DNS Server(Bind)的 IPv6 設定 ✧ WEB Server(Apache)的 IPv6 設定
16:00 – 16:30	Q&A

DNS教育訓練

1

DNS基礎概念

2

網域名稱是什麼？

- 網域名稱是企業或個人在網路上的身份，
 - 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

3

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18類
 - <http://www.iana.org/gtld/gtld.htm>
 - ccTLDs:
 - tw/cn/jp/us 共 248 個
 - <http://www.iana.org/cctld/cctld-whois.htm>
 - 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
- TWNIC 於2005/11/1 開放泛英(xxx.tw) 申請
- ICANN於2011/6通過開放TLD申請

4

DNS 背景介紹

- 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

/etc/hosts

- 1984年Paul Mockapetris 建立了第一個 DNS 的規範(RFC1034， RFC1035)

- 85 年隨即出現了第一個網域名稱

5

域名與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

6

DNS 運作模式

- 名稱查詢之服務
- 分散式
 - 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
 - 全球最大的分散式資料庫系統
 - 以樹狀結構的方式找到目的位址(每個結點需要授權)
 - <http://www.root-servers.org/> 目前 Root Server 分布情形
- 穩定
 - 負載平衡:可由 Master 主機自由的複製到 Slave 主機
 - 備援:一個網域名稱可有多台主機共同服務(輪流查詢)
- 樹狀結構
 - 經由全球唯一的 Root Server 達到正確搜尋的目的
 - Root Server 共十三部，每一部可能都有許多 Mirror (如 f.root-servers.net 有二三十部)
- 效率
 - 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

7

Root Server 共十三部

```
[root@localhost ~]# dig
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5 <<>>
;; global options: printCmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18432
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;;                               IN      NS
;; ANSWER SECTION:
;      175287 IN      NS      b.root-servers.net.
;      175287 IN      NS      k.root-servers.net.
;      175287 IN      NS      f.root-servers.net.
;      175287 IN      NS      e.root-servers.net.
;      175287 IN      NS      d.root-servers.net.
;      175287 IN      NS      g.root-servers.net.
;      175287 IN      NS      c.root-servers.net.
;      175287 IN      NS      a.root-servers.net.
;      175287 IN      NS      j.root-servers.net.
;      175287 IN      NS      m.root-servers.net.
;      175287 IN      NS      h.root-servers.net.
;      175287 IN      NS      i.root-servers.net.
;      175287 IN      NS      l.root-servers.net.
;; Query time: 4 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Sat May 30 23:01:53 2015
;; MSG SIZE rcvd: 228
[root@localhost ~]#
```

DNS 名稱表示法

Fully Qualified Domain Name (FQDN)

WWW.EP.NET.

注意結尾的點

- 每一個名稱間以 . 隔開
- 一個 FQDN 可以對應到不同的位置或服務
 - 一個名稱對應到多個 IP 稱為 Round Robin
 - 一個名稱對應到不同的服務如 MX
- 每個 FQDN 如同 IP 一般皆具有唯一性
- 其限制
 - 最多 127 層
 - 每個分支最長 63 字元 (a-z, 0-9, -)
 - 總長 255 字元

9

小範圍

大範圍

www.slhs.tp.edu.tw.

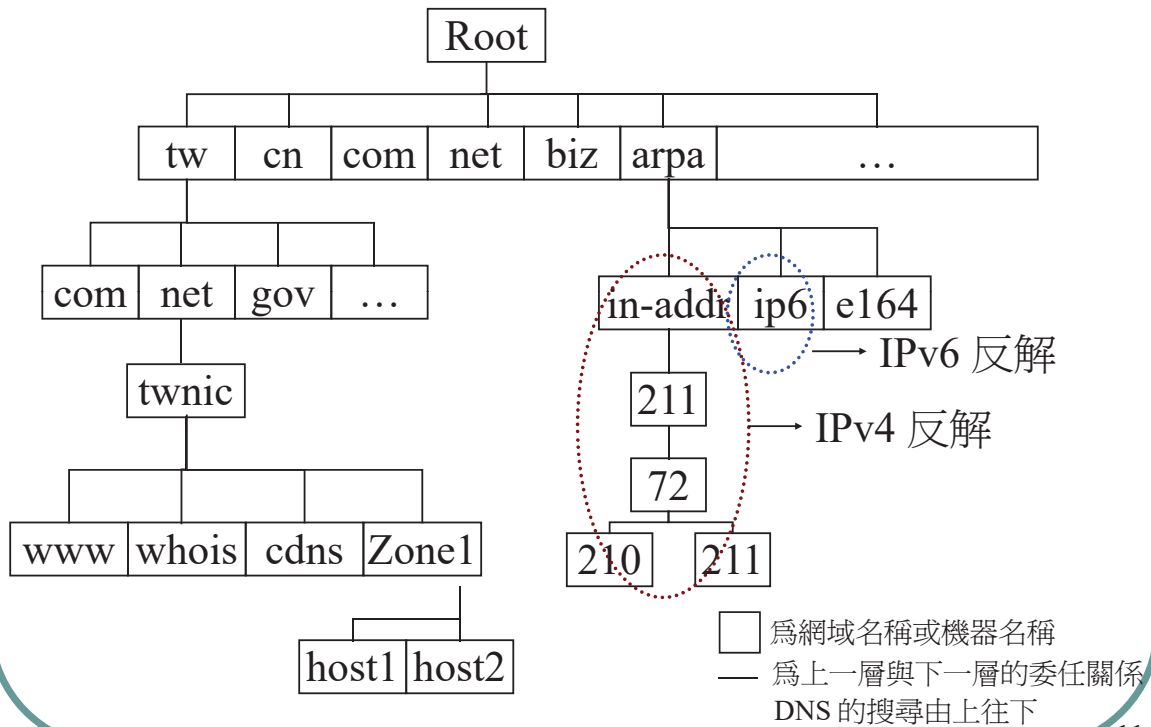
書寫方向

大範圍

小範圍

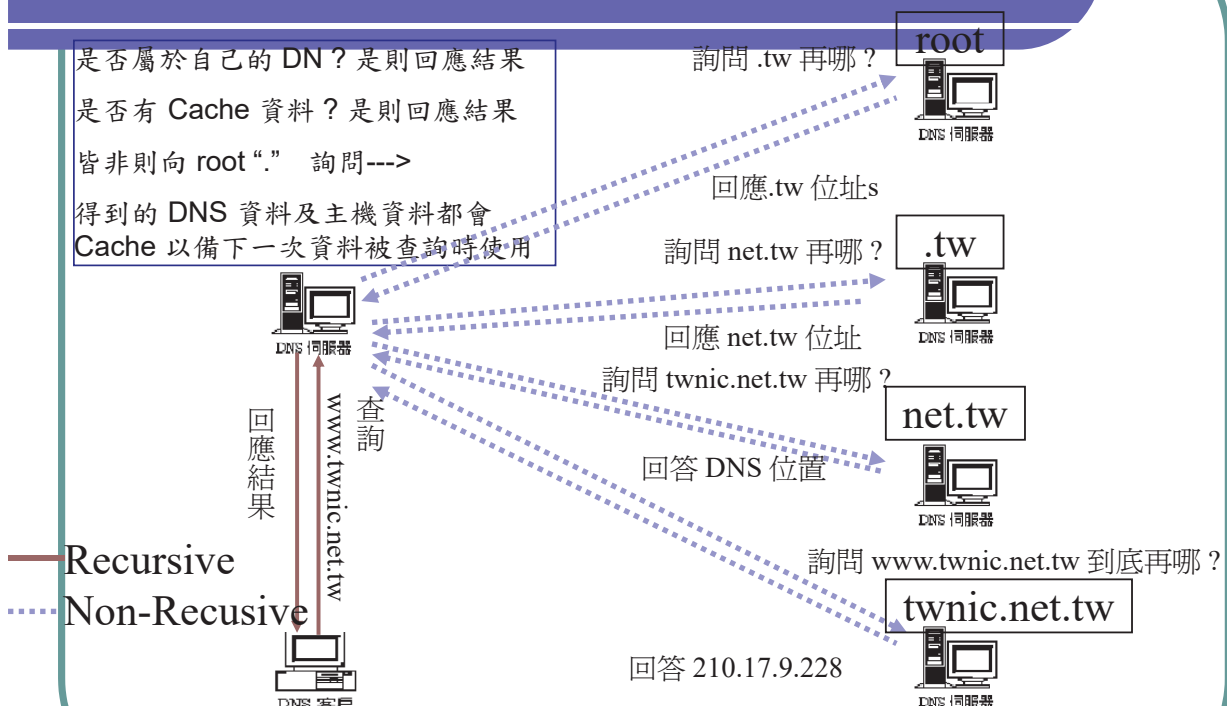
203.72.185.3

DNS 樹狀結構



11

運作原理 圖示



12

運作原理(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

13

運作原理(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

14

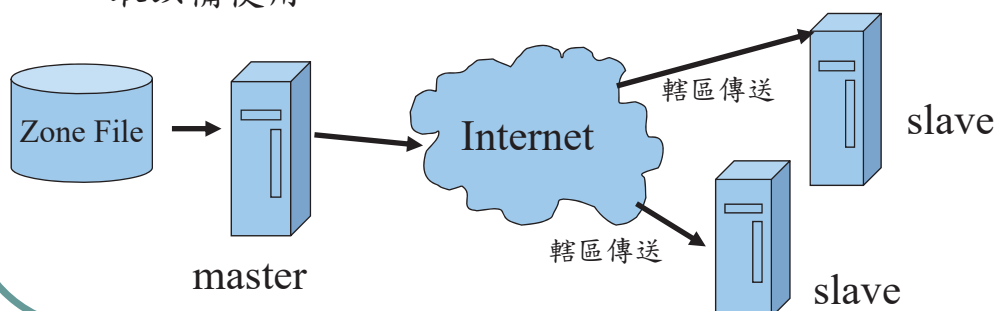
DNS 的平台

- LINUX
 - 常見為ISC BIND
 - 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,並持續更新
 - Bind 可於 Windows 上運作

15

名稱伺服器類型

- 權威主機(Authoritative)
 - 可管理或回答其網域名稱之答案
 - Master 主機指 DNS 所管轄的資料是從檔案 (Zone File) 中而來 (twnic.net.tw)
 - Slave 主機指 DNS 所管轄的資料是以轄區傳送(Zone Transfer) 從 Master 而來 (ns.twnic.tw)
- Cache-Only 主機 (168.95.1.1)
 - 即沒有管理任何的網域名稱，接受查詢與回應並將其快取以備使用



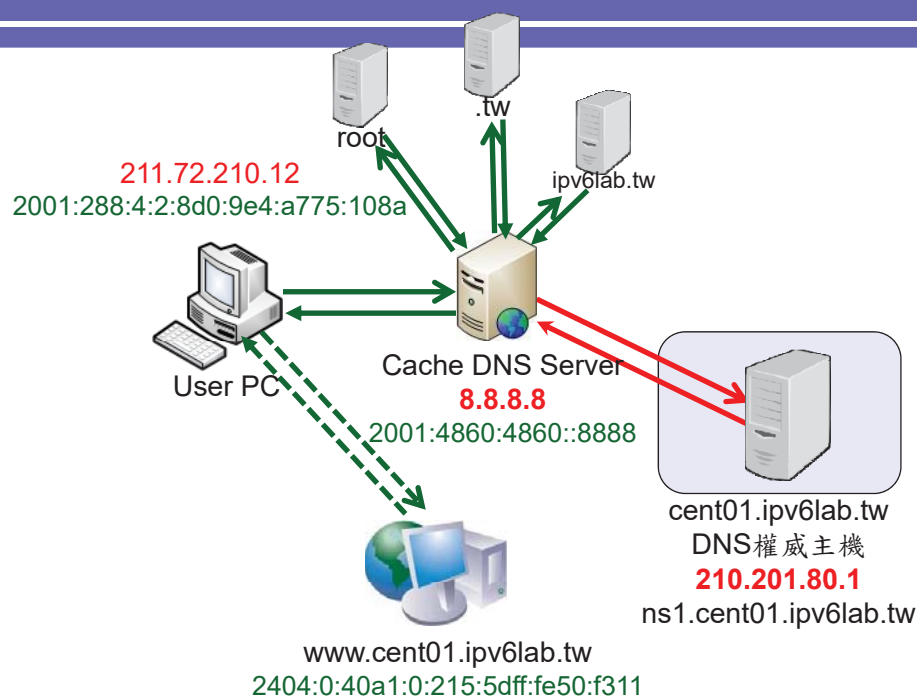
16

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
 - 反解的 DNS Query 遠比正解高出許多
 - 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

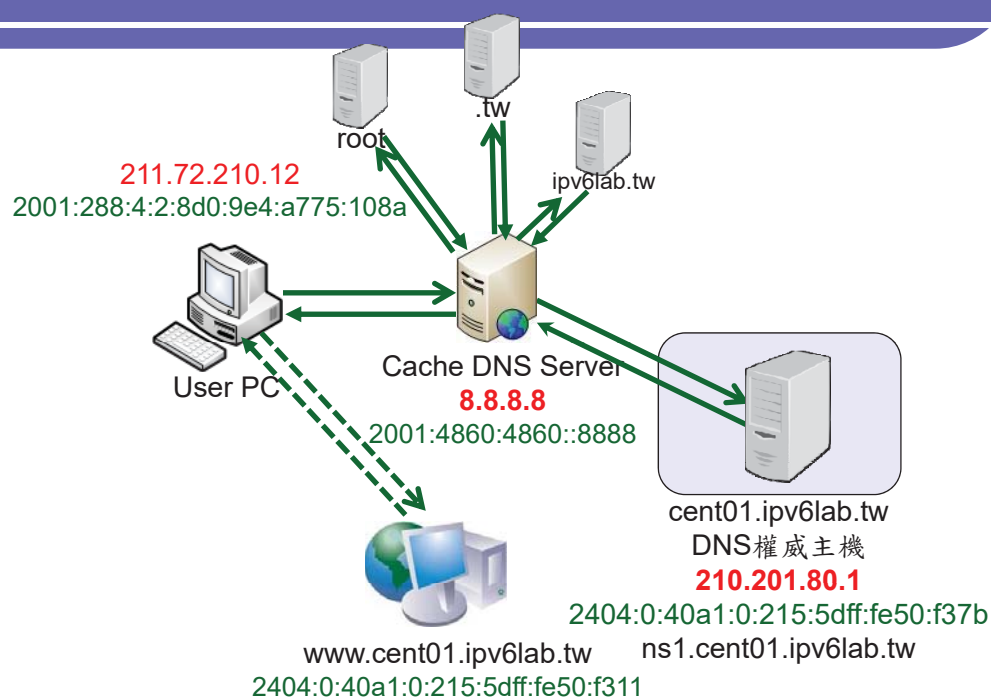
17

DNS權威主機只支援IPv4



18

DNS權威主機支援IPv4及IPv6



19

常見DNS記錄類型

代碼	號碼	定義的 RFC	描述	功能
A	1	RFC 1035	IPv4 IP 位址記錄	傳回一個 32 位元的 IPv4 位址，最常用於對映主機名稱到 IP 位址。
AAAA	28	RFC 3596	IPv6 IP 位址記錄	傳回一個 128 位元的 IPv6 位址，最常用於對映主機名稱到 IP 位址。
NS	2	RFC 1035	名稱伺服器記錄	委託 DNS 區域 (DNS zone) 使用已提供的權威域名伺服器。
PTR	12	RFC 1035	指標記錄	用來執行反向 DNS 查找
SOA	6	RFC 1035	權威記錄的起始	指定有關 DNS 區域的權威性資訊，包含主要名稱伺服器、域名管理員的電郵地址、域名的流水式編號、和幾個有關重新整理區域的定時器。

正向查詢(正解)DNS Record

- \$ORIGIN cent01.ipv6lab.tw.
- IPv4 **A** Record
 - ns1 IN A 210.201.80.1
 - www IN A 210.201.80.1
- IPv6 **AAAA** Record
 - ns1 IN AAAA 2404:0:40a1:0:215:5dff:fe50:f37b
 - www IN AAAA 2404:0:40a1:0:215:5dff:fe50:f37b
 - www IN AAAA 2600::3

反向查詢(反解)DNS Record

- IPv4 **PTR** Record #210.201.80.1
- \$ORIGIN 80.201.210.in-addr.arpa.
 - 1 IN PTR ns1.cent01.ipv6lab.tw.
 - 1 IN PTR www.cent01.ipv6lab.tw.
- IPv6 **PTR** Record #2404:0:40a1:0:215:5dff:fe50:f37b
- \$ORIGIN 0.0.0.0.1.a.0.4.0.0.0.0.4.0.4.2.ip6.arpa.
 - b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0 IN PTR ns1.cent01.ipv6lab.tw.
 - b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0 IN PTR www.cent01.ipv6lab.tw.



THANK YOU

IPV6作業系統與應用服務建置 (WINDOWS)



點進網域新視界！

1



Windows Server 2012 升級IPv6
實作教學—Server設定IPv6位址與連線、DNS
Server升級IPv6、Web Server升級IPv6

2

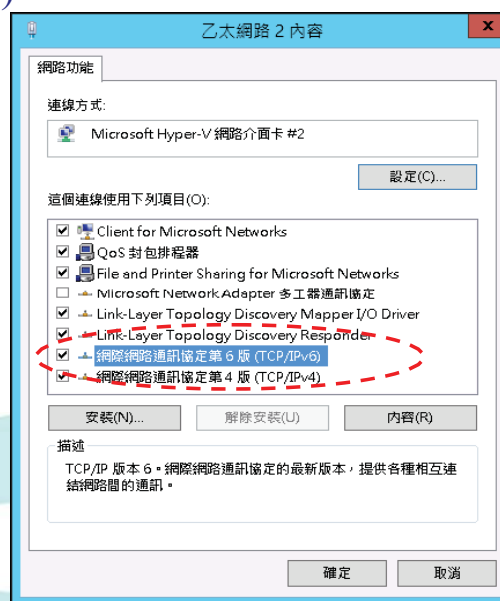
Windows Server 2012 啟動 IPv6 通訊協定(1/3)

- Windows Server 2012 啟動 IPv6 通訊協定：
Windows Server 2012 作業系統已經預設啟動『網際網路通訊協定第 6 版 (TCP/IPv6)』，因此在安裝完 Windows Server 2012 作業系統後，不需要再執行手動啟動 IPv6 連線的程序
- 如果要手動關閉 IPv6 能力或再次檢查 IPv6 是否已經啟動，則可以透過圖形介面(Graphical User Interface, GUI)進行

Windows Server 2012 啟動

IPv6 通訊協定(2/3)

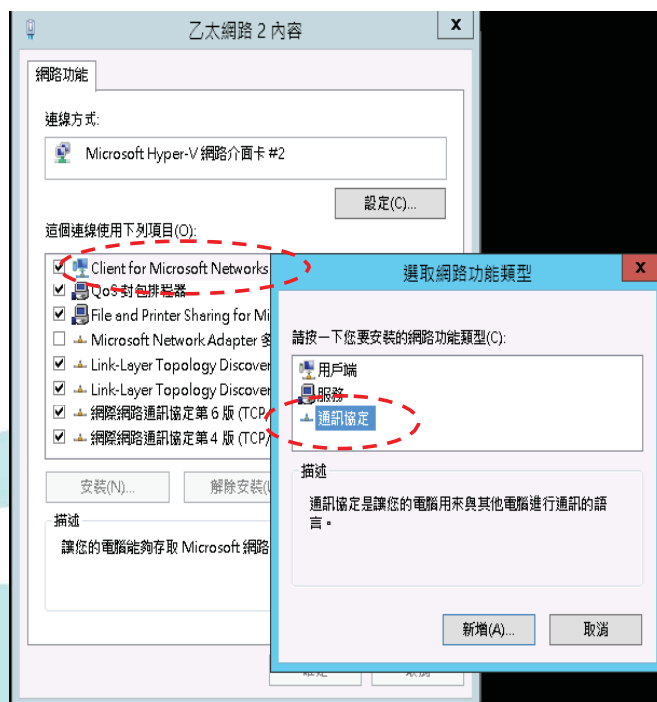
- 檢查 IPv6 是否已經啟動
 - 從『開始』→『控制台』→『網路連線』
 - 在『區域連線 內容』視窗中，如已出現『網際網路通訊協定第 6 版 (TCP/IPv6)』則 IPv6 已經啟動



Windows Server 2012 預設支援 IPv6

Windows Server 2012 啟動 IPv6 通訊協定(3/3)

- 利用圖形化介面啟動 IPv6
 - ：如果尚未安裝 IPv6 通訊協定，則安裝步驟如下
 - 從『開始』→『控制台』→『網路與網際網路』→『網路和共用中心』
 - 在『區域連線』→『內容』視窗中選取『Client for Microsoft Networks』，並且按下『安裝』
 - 在跳出的『選取網路功能類型』視窗中，選取『通訊協定』並按下新增。接著在跳出的『選取網路通訊協定』視窗中選取『Microsoft TCP/IP version 6』，接著按下『確定』

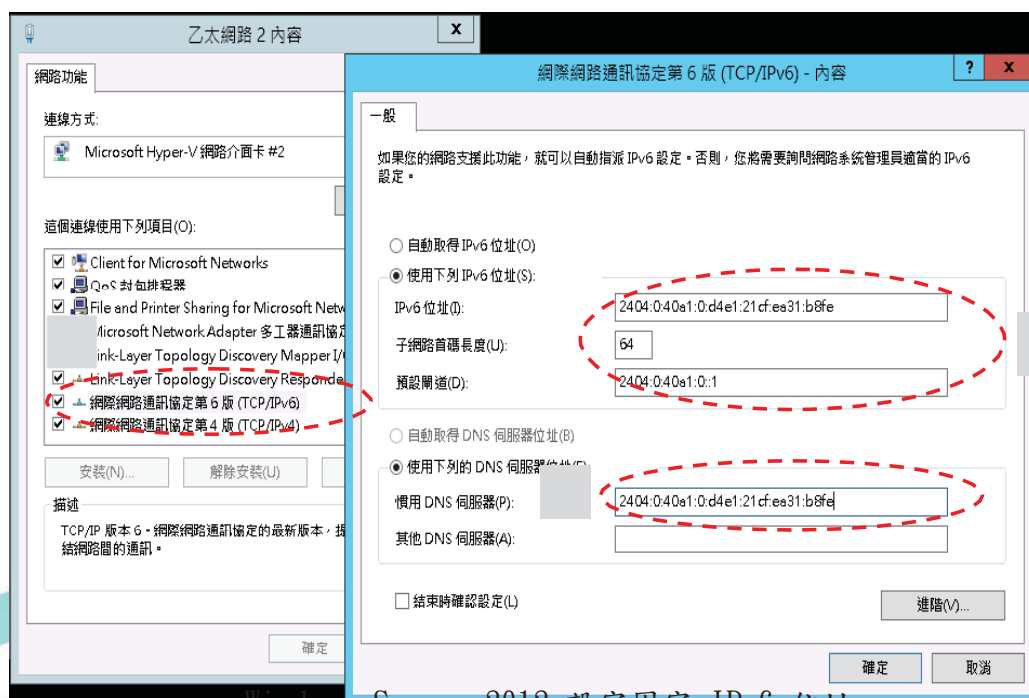


Windows Server 2012 圖形化介面啟動支援 IPv6

設定 Windows Server 2012 主機 IPv6 位址(1/4)

- 設定主機 IPv6 位址：透過圖形化界面設定 IPv6 位址，設定步驟如下
 - 從『開始』→『控制台』→『網路與網際網路』→『網路和共用中心』
 - 在『區域連線』在『內容』視窗中選取『網際網路通訊協定第 6 版(TCP/IPv6)』，接著按下『內容』
 - 在跳出的『網際網路通訊協定第 6 版 (TCP/IPv6) – 內容』視窗中 進行手動設定 IPv6 位址，設定步驟如下
 - 點選『使用下列 IPv6 位址(S):』選項
 - 在 IPv6 位址欄位中輸入欲使用的 IPv6 位址
 - 在『子網路首碼長度(U):』欄位中輸入 Prefix 長度
 - 輸入預設閘道
 - 輸入慣用 DNS 伺服器位址

設定 Windows Server 2012 主機 IPv6 位址(2/4)



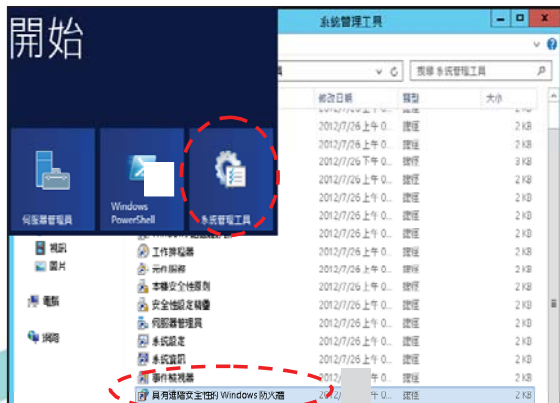
Windows Server 2012 設定固定 IPv6 位址

設定 Windows Server 2012 主機 IPv6 位址(3/4)

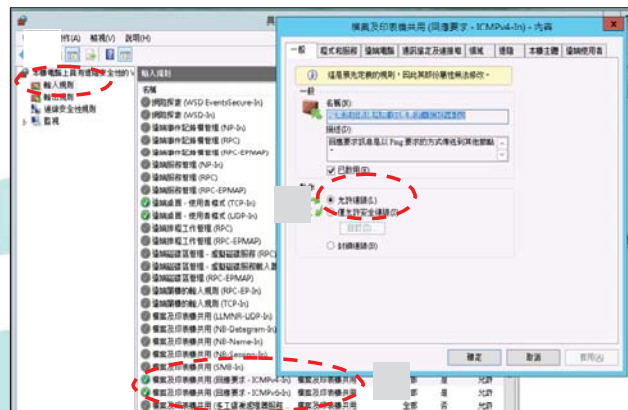
- Windows 防火牆開啟 ICMP Ping：Windows Server 2012 的防火牆預設是關閉 Ping 的回應，開放 Ping 的回應不是必要的設定，有可能基於安全性考量而特意關閉。如果要從其他電腦對主機做 Ping 測試，則要修改設定，步驟如下
 - 以系統管理員權限登入 Windows Server 2012
 - 從『開始』→『系統管理工具』在『具有進階安全性的 Windows 防火牆』。請注意，如果不是以系統管理員權限登入，就不會有這個功能項目

設定 Windows Server 2012 主機 IPv6 位址(4/4)

- ❑ 點選『輸入規則』→『檔案及印表機共用(回應要求-ICMPv4-In)』→勾選『已啟用』在『確定』，開啟 IPv4 Ping 回應，如圖 6。
- ❑ 點選『輸入規則』→『檔案及印表機共用(回應要求-ICMPv6-In)』→勾選『已啟用』→『確定』，開啟 IPv6 Ping 回應。



具有進階安全性的 Windows 防火牆



Windows 防火牆開啟 ICMP Ping

驗證 IPv6 通訊協定(1/5)

● 驗證啟動 IPv6 通訊協定

- ❑ 驗證啟動 IPv6 通訊協定：在 Windows server 2012 主機藉由命令提示字元模式使用『ping』指令，察看是否有回應，確認主機已啟動支援 IPv6 通訊協定

- ❑ Comm


```
C:\Users\Administrator>ping -6 ::1

Ping ::1 (使用 32 位元組的資料):
回覆自 ::1: 時間<1ms
回覆自 ::1: 時間<1ms
回覆自 ::1: 時間<1ms
回覆自 ::1: 時間<1ms

::1 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms
```

C:\Users\Administrator>

Windows 2012 Server 檢測 IPv6 位址已啟動

驗證 IPv6 通訊協定(2/5)

- 驗證 IPv6 位址：在 Windows server 2012 主機藉由命令提示字元模式使用『ipconfig』指令

驗 C:\Users\Administrator> ipconfig

□ Windows IP 設定

乙太網路卡 乙太網路 2:

連線特定 DNS 尾碼 :

IPv6 位址 : 2404:0:40a1:0:5026:28ba:59ab:f0c9

連結-本機 IPv6 位址 : fe80::5026:28ba:59ab:f0c9%15

IPv4 位址 : 210.201.80.171

子網路遮罩 : 255.255.255.0

預設閘道 : fe80::7a19:f7ff:fe88:de81%15

11

驗證 IPv6 通訊協定(3/5)

2404:0:40a1::1

210.201.80.254

通道介面卡 isatap.{51BD53A2-A1E2-44BD-B0B8-46CE1F02FCC9}:

媒體狀態 : 媒體已中斷連線

連線特定 DNS 尾碼 :

通道介面卡 區域連線* 9:

連線特定 DNS 尾碼 :

IPv6 位址 : 2001:0:4137:9e76:1c6d:2b62:2d36:af54

連結-本機 IPv6 位址 : fe80::1c6d:2b62:2d36:af54%14

預設閘道 :

PS C:\Users\Administrator>

Windows Server 2012 顯示 IPv6 位址

12

驗證 IPv6 通訊協定(4/5)

- 驗證對外 IPv6 連線：在 Windows server 2012 主機藉由命令提示字元模式使用『ping』指令，查看是否有回應，以確認 Windows Server 2012 主機是否已經可以連接到外界之 IPv6 網路。測試用 IPv6 網站可選 www.ipv6.org.tw 或其他 IPv6 網站
- Command：ping -6 www.ipv6.org.tw

```
C:\Users\Administrator>ping -6 www.ipv6.org.tw

Ping www.ipv6.org.tw [2001:c50:ffff:1:21a:92ff:fe43:d665] (使用 32 位元組的資料):
回覆自 2001:c50:ffff:1:21a:92ff:fe43:d665: 時間=4ms
回覆自 2001:c50:ffff:1:21a:92ff:fe43:d665: 時間=2ms
回覆自 2001:c50:ffff:1:21a:92ff:fe43:d665: 時間=2ms
回覆自 2001:c50:ffff:1:21a:92ff:fe43:d665: 時間=2ms

2001:c50:ffff:1:21a:92ff:fe43:d665 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 2ms, 最大值 = 4ms, 平均 = 2ms

C:\Users\Administrator>
```

Windows 2012 Server 檢測主機連接外界 IPv6 網站

13

驗證 IPv6 通訊協定(5/5)

- 從測試用戶端 Ping 主機：如果要從其他電腦對主機做 Ping 測試，要先確定主機的防火牆已經打開『允許傳入的回應要求』。在

<pre>C:\Users\Administrator>ping -4 210.201.80.171 Ping 210.201.80.171 (使用 32 位元組的資料): 回覆自 210.201.80.171: 位元組=32 時間<1ms TTL=128 回覆自 210.201.80.171: 位元組=32 時間<1ms TTL=128 回覆自 210.201.80.171: 位元組=32 時間<1ms TTL=128 回覆自 210.201.80.171: 位元組=32 時間<1ms TTL=128 210.201.80.171 的 Ping 統計資料: 封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失), 大約的來回時間 (毫秒): 最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms</pre>	<pre>C:\Users\Administrator>ping -6 2404:0:40a1:0:5026:28ba:59ab:f0c9 Ping 2404:0:40a1:0:5026:28ba:59ab:f0c9 (使用 32 位元組的資料): 回覆自 2404:0:40a1:0:5026:28ba:59ab:f0c9: 時間<1ms 回覆自 2404:0:40a1:0:5026:28ba:59ab:f0c9: 時間<1ms 回覆自 2404:0:40a1:0:5026:28ba:59ab:f0c9: 時間<1ms 回覆自 2404:0:40a1:0:5026:28ba:59ab:f0c9: 時間<1ms 2404:0:40a1:0:5026:28ba:59ab:f0c9 的 Ping 統計資料: 封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失), 大約的來回時間 (毫秒): 最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms</pre>
---	--

從測試用戶端 Ping 主機

14

Windows Server 2012 DNS 伺服器啟動支援 IPv6(1/6)

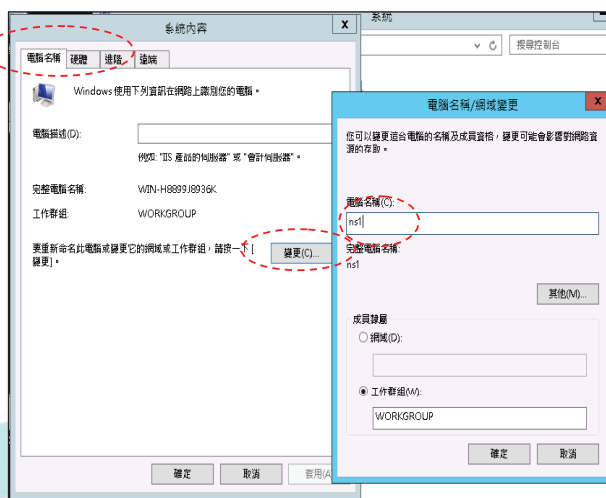
- 安裝及設定 DNS 伺服器：在 Windows Server 2012 主機建立 IPv6 連線能力後，接著設定內建的 DNS 伺服器，並驗證 DNS 伺服器可提供 IPv6 網域名稱查詢服務。安裝 DNS 伺服器的方式可透過圖形介面新增 IIS 角色，以下為安裝 DNS 伺服器的步驟，如果主機原本就已經提供 DNS 服務，則可以跳過安裝的步驟直接進行設定

15

Windows Server 2012 DNS 伺服器啟動支援 IPv6(2/6)

- 修改主機電腦名稱和網域：先依據預定要建立的 DNS 完整主機網域名稱修改電腦名稱和網域名稱，網域名稱系統採用階層式架構，電腦名稱修改的步驟為：

- 『我的電腦』→右鍵→『內容』在選擇『電腦名稱』→按『變更』→電腦名稱輸入『ns1』



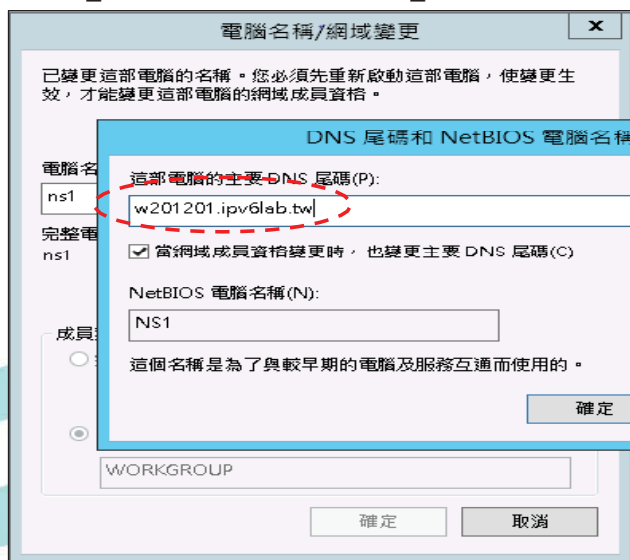
修改主機電腦名稱和網域

16

Windows Server 2012 DNS 伺服器啟動支援 IPv6(3/6)

伺服器啟動支援 IPv6(3/6)

- 繼續選擇『其他』在主要 DNS 尾碼處輸入『繼續選擇『其他』→主要DNS 尾碼處輸入『w201201.ipv6lab.tw』→連按『確定』，並重新開機



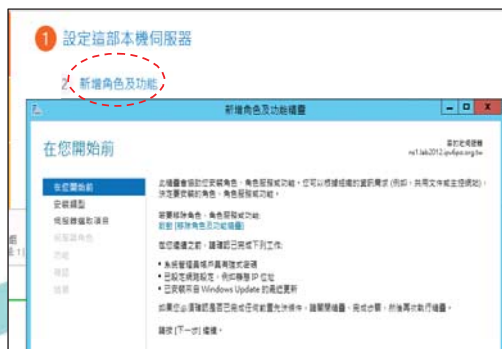
設定主要 DNS 尾碼

17

Windows Server 2012 DNS 伺服器啟動支援 IPv6(4/6)

伺服器啟動支援 IPv6(4/6)

- 使用圖形介面新增伺服器角色：安裝 DNS 伺服器時，可透過圖形介面新增伺服器角色
 - 『新增角色及功能』→『下一步』→『角色型或功能型安裝』→『下一步』
 - 選取『下一步』→『DNS 伺服器』→『新增功能』→『下一步』→『下一步』→『安裝』，接下來會花一段時間安裝 DNS 伺服器



新增伺服器角色

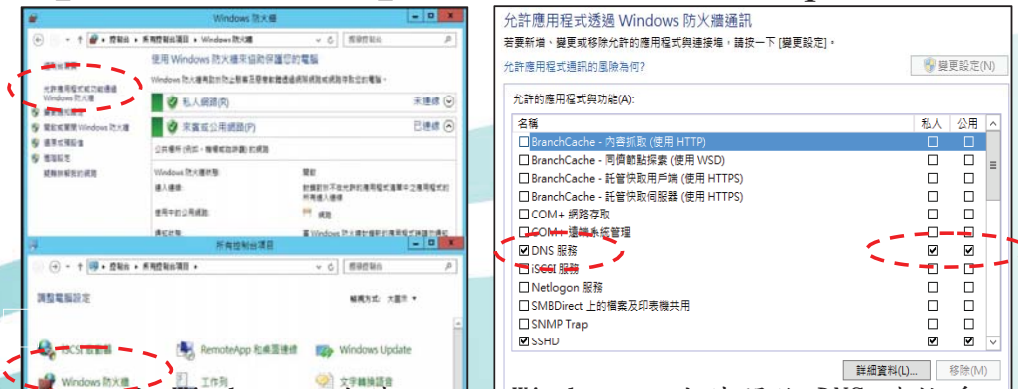


新增 DNS 伺服器角色

18

Windows Server 2012 DNS 伺服器啟動支援 IPv6(5/6)

- 確認防火牆開啟 UDP port 53-安裝 DNS 伺服器後 Windows Server 2012 的防火牆會自動開啟 DNS 使用的 UDP port 53，可以透過以下步驟確認或調整：
 - ❑ 『開始』→『控制台』→『Windows 防火牆』
 - ❑ 點選左上方『允許程式或功能通過 Windows 防火牆』→『DNS 服務』要勾選以打開 UDP port 53



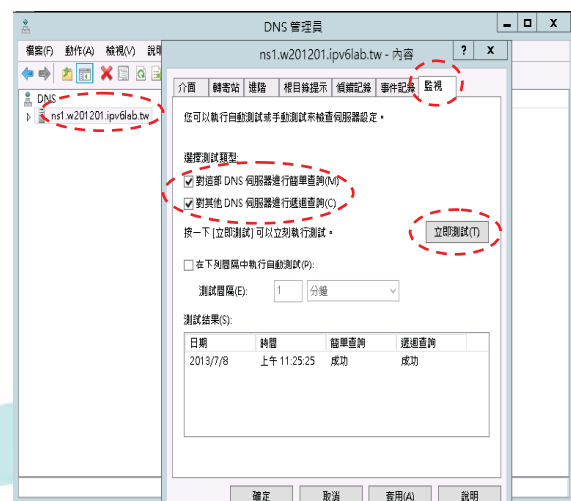
設定 Windows 防火牆

Windows 防火牆開啟 DNS 連接埠

19

Windows Server 2012 DNS 伺服器啟動支援 IPv6(6/6)

- 對 DNS 伺服器進行名稱解析測試
 - ❑ 『開始』→『系統管理工具』→『伺服器管理員』，在 DNS 下電腦名稱『ns1』上按右鍵→選取『內容』
 - ❑ 選擇『監視』並將『對這部 DNS 伺服器進行簡單查詢』及『對其他 DNS 伺服器進行遞迴查詢』打勾核取並按『立即測試』，

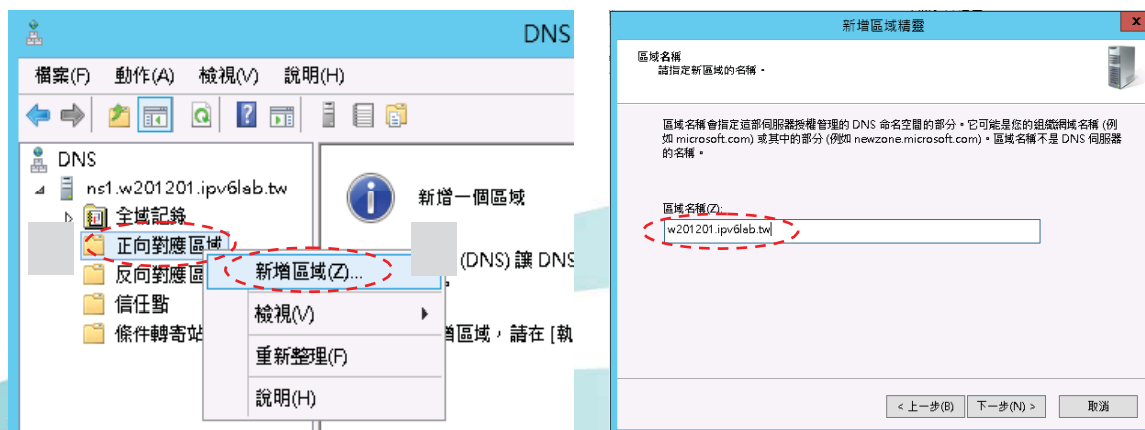


對 DNS 伺服器進行簡單查詢測試

20

設定 DNS IPv4 A 紀錄(1/12)

- 新增正向對應區域(Zone)
 - 『開始』→『系統管理工具』→『DNS』，啟動 DNS 管理員
 - 點選『正向對應區域』→『新增區域』，啟動新增區域精靈
 - 點選『下一步』→『主要區域』→『下一步』在輸入想設定的網域名稱



新增正向區域

輸入網域名稱

21

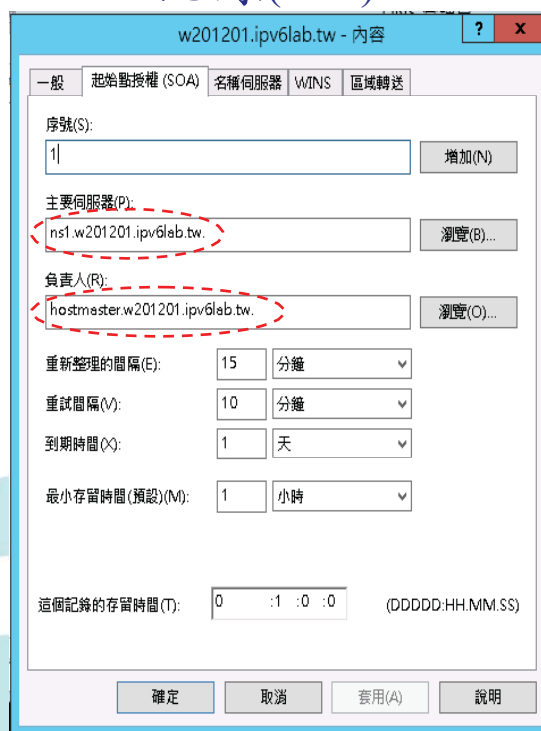
設定 DNS IPv4 A 紀錄(2/12)

- 接下來依序依照畫面指引完成各項設定：
 - 區域檔案：輸入網域要存的檔名，可任意取名，預設會是區域名稱後面加上.dns，我們用預設並按下一步，如果要使用其他 DNS 伺服器的設定檔，請選「使用現存檔案」並先將已有的設定檔複製到 Windows 目錄\system32\dns
 - 動態更新：選擇『不允許動態更新』完全由手動新增 DNS 記錄

22

設定 DNS IPv4 A 紀錄(3/12)

- 修訂正向區域的 SOA 記錄：在 DNS 管理員右方視窗『起始點授權 (SOA)』上快按選滑鼠 2 次 → 點選『啟動授權 (SOA)』在『負責人』填入管理者 E-mail，”@” 以 ”.” 代替，最後也加一個 ”.”，例如 hostmaster@w201201.ipv6lab.tw 則輸入『hostmaster.w201201.ipv6lab.tw.』

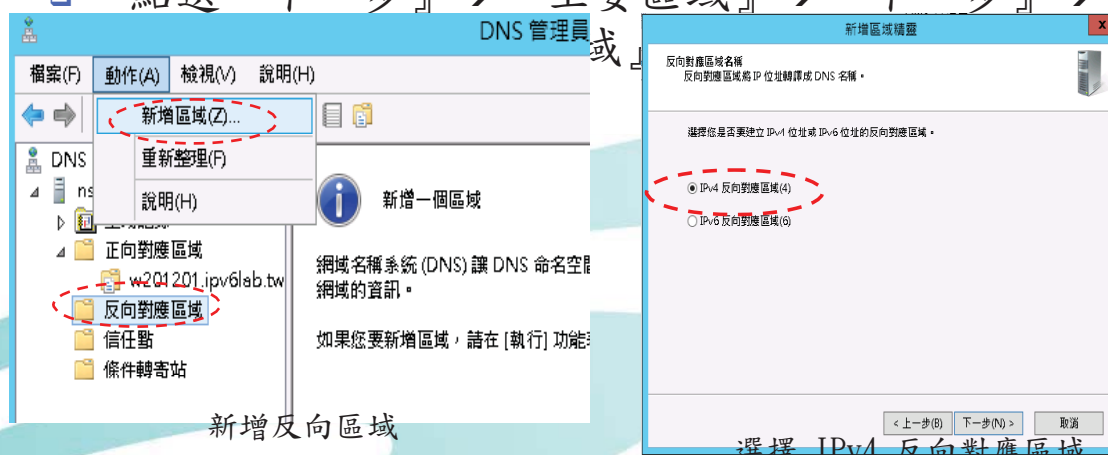


修改正向區域的 SOA 記錄

23

設定 DNS IPv4 A 紀錄(4/12)

- 設定反向對應區域(Reverse Zone)
 - 從 DNS 的管理員左方視窗點選『反向對應區域』 → 『新增區域』，啟動新增區域精靈
 - 點選『下一步』 → 『主要區域』 → 『下一步』 →

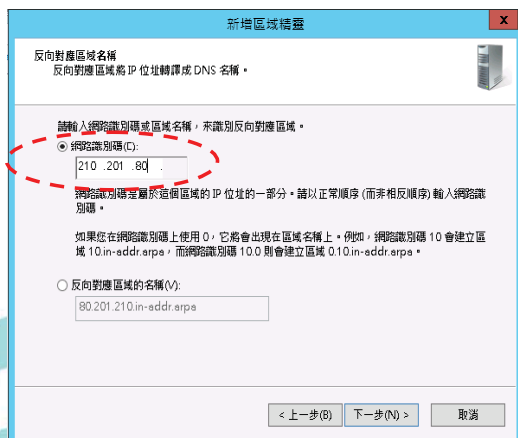


新增反向區域

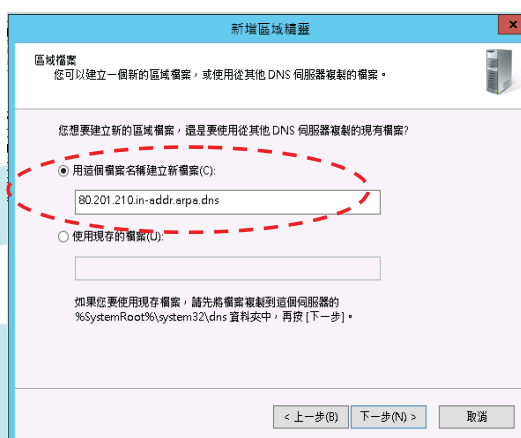
選擇 IPv4 反向對應區域

設定 DNS IPv4 A 紀錄(5/12)

- 在『網路識別碼』輸入 IPv4 網段前 3 碼，例如 210.201.80.0/24 則輸入『210.201.80』
- 區域檔案名稱：系統預設取 IP 網段前 3 碼倒過來再加上 in-addr.arpa→動態更新：選擇『不允許動態更新』讓我們完全由手動新增記錄→完成反向區域設定



反向區域設定網路識別碼



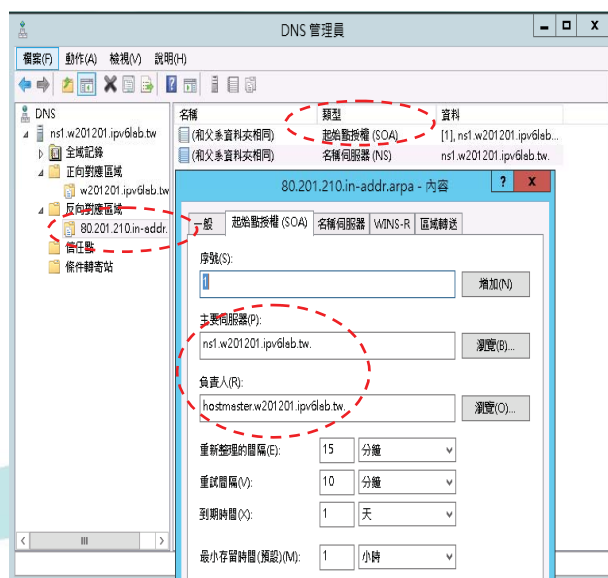
設定反向區域檔案名稱

25

設定 DNS IPv4 A 紀錄(6/12)

- 確認反向區域的 SOA 及 NS 記錄

- 點選 DNS 管理員左方視窗建立的反向對應區域在右方視窗『起始點授權 (SOA)』上快按選滑鼠 2 次在點選『起始點授權 (SOA)』→確認『主要伺服器』已輸入主機全名(最後加一個".")
- 在『負責人』確認管理者 E-mail，"@" 以 "." 代替，最後也加一個 "."，例如 hostmaster@w201201.ipv6lab.tw 則輸入『hostmaster.w201201.ipv6lab.tw.』

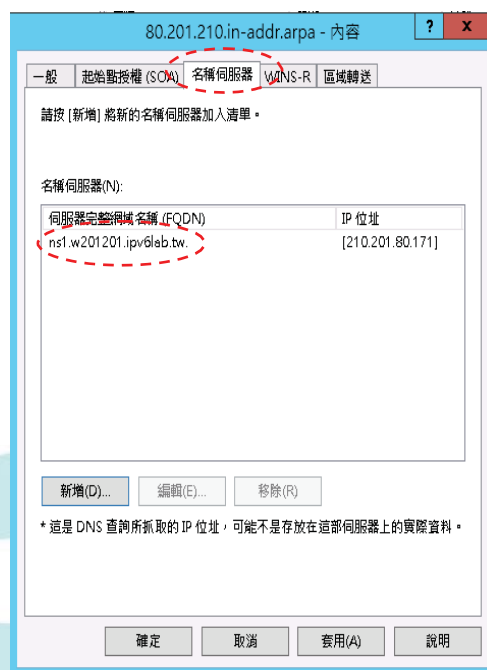


確認反向區域的 SOA 記錄

26

設定 DNS IPv4 A 紀錄(7/12)

- 點選『名稱伺服器』→
確認伺服器完整網域名
稱 (FQDN)，本例為『
ns1.w201201.ipv6lab.tw.
』，最後面有一個 ”
.” → 在『IP 位址』確認
DNS 主機的 IP 『
210.201.80.171』



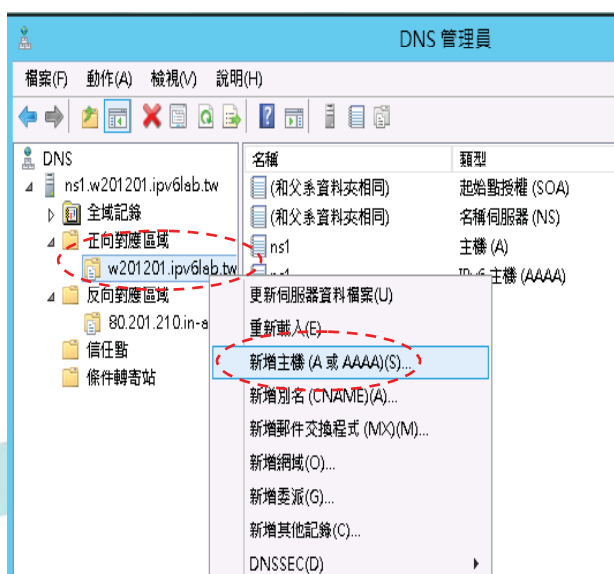
確認反向區域的 NS 記錄

27

設定 DNS IPv4 A 紀錄(8/12)

- 設定主機正向對應紀錄(A Record)

- 新增 DNS 主機正向
解析對應紀錄在 DNS
管理員視窗正向對應
區域，點選先前新增
的區域『
w201201.ipv6lab.tw』
→ 點選滑鼠『右鍵』
→ 選擇『新增主機』

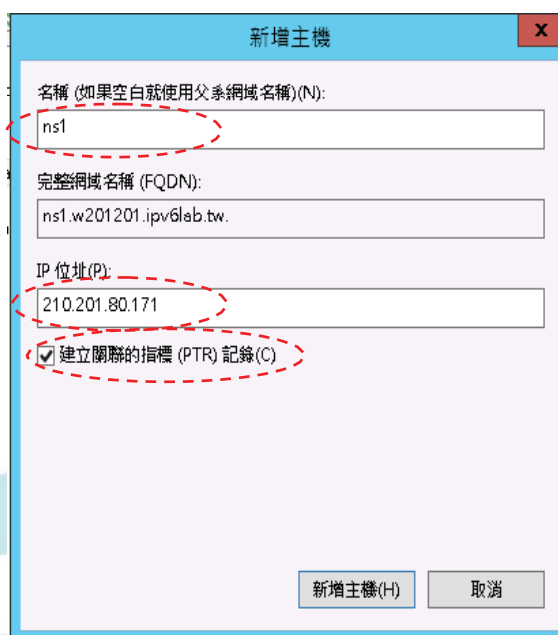


新增其他主機 A Record

28

設定 DNS IPv4 A 紀錄(9/12)

- 新增 DNS 主機正向解析對應紀錄：在完成新增正向對應區域後，DNS 主機的正向解析對應紀錄 ns1 應該已經自動建立。如果沒有出現，可以手動新增：名稱輸入『www』，下方自動出現完整網域名稱『ns1.w201201.ipv6lab.tw.』在輸入 DNS 主機位址，本例為『210.201.80.171』在勾選『建立關聯的 PTR 記錄』→『新增主機』，如圖 40，反查記錄將會自動建立



新增主機

名稱 (如果空白就使用父系網域名稱)(N):
ns1

完整網域名稱 (FQDN):
ns1.w201201.ipv6lab.tw.

IP 位址(P):
210.201.80.171

☒ 建立關聯的指標 (PTR) 記錄(C)

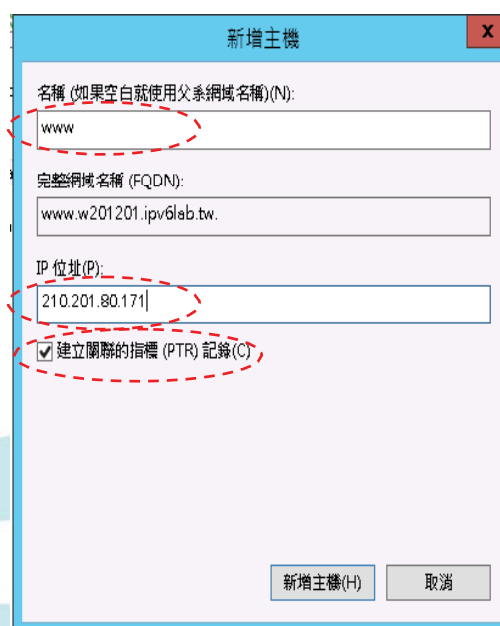
新增主機(H) 取消

新增 DNS 主機 A Record 的網域名稱及 IP 位址

29

設定 DNS IPv4 A 紀錄(10/12)

- 新增 WWW 主機正向解析對應紀錄：接著為 WWW 主機建立正向解析對應紀錄：名稱輸入『www』，下方自動出現完整網域名稱『www.w201201.ipv6lab.tw.』在輸入 WWW 主機位址，本例為『210.201.80.171』在勾選『建立關聯的 PTR 記錄』→『新增主機』，反查記錄將會自動建立



新增主機

名稱 (如果空白就使用父系網域名稱)(N):
www

完整網域名稱 (FQDN):
www.w201201.ipv6lab.tw.

IP 位址(P):
210.201.80.171

☒ 建立關聯的指標 (PTR) 記錄(C)

新增主機(H) 取消

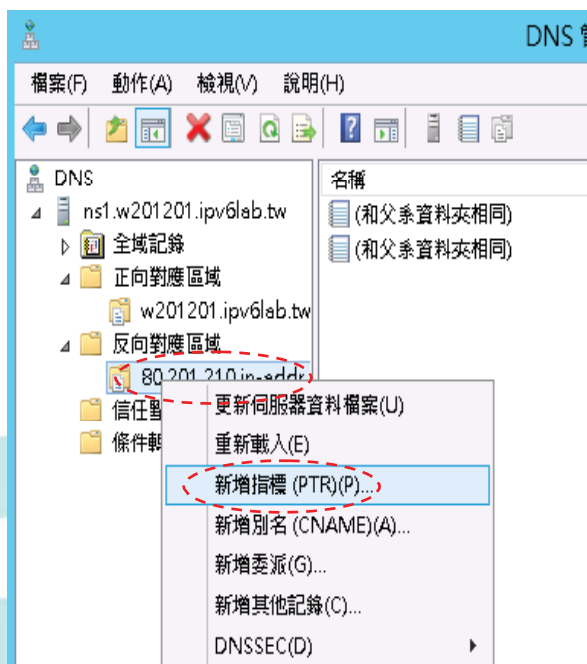
新增 www 主機 A Record 的網域名稱及 IP 位址

30

設定 DNS IPv4 A 紀錄(11/12)

- 設定主機反向對應紀錄 (PTR Record)：在反向對應區域如果看不到自動產生的 PTR 記錄，請先按滑鼠『右鍵』選擇『重新整理』。如果還是沒有，就手動新增指標 (PTR)，步驟如下：

- 點選『反向對應區域』再點選『80.201.210.in-addr.arpa.dns』→滑鼠『右鍵』在選擇『新增指標 (PTR)』

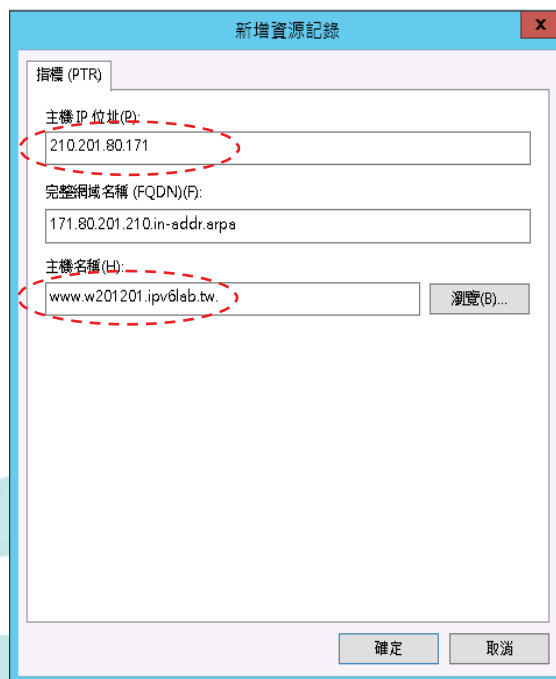


新增指標 (PTR) 反查

31

設定 DNS IPv4 A 紀錄(12/12)

- 主機 IP 位址輸入
www 主機位址，本例為『210.201.80.171』
→主機名稱輸入『www.w201201.ipv6lab.tw.』，最後有一個”.”



新增指標 (PTR) 反查的 IP 位址及主機名稱

32

檢測 DNS IPv4 A 設定(1/3)

使用 nslookup 指令檢查 dns 設定是否正常，以下示範使用 Windows 8 做為測試端電腦。操作過程出現如 Non-existent domain，表示 DNS 找不到查詢的資料，請檢查 DNS 設定

● 使用 nslookup 進行查詢

```
PS C:\Users\Administrator> nslookup // 使用 nslookup 命令查詢
預設伺服器: UnKnown
Address: 2404:0:40a1:0:5026:28ba:59ab:f0c9

> server ns1.w201201.ipv6lab.tw // 指定 DNS 查詢主機
預設伺服器: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171
```

使用 nslookup 進行查詢

33

檢測 DNS IPv4 A 設定(2/3)

```
● ] > set type=a // 指定查詢 A 紀錄
> ns1.w201201.ipv6lab.tw // 輸入要查詢的網址
伺服器: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171

名稱: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171 // 回應的 IPv4 位址

> www.w201201.ipv6lab.tw // 輸入要查詢的網址
伺服器: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171

名稱: www.w201201.ipv6lab.tw
Address: 210.201.80.171 // 回應的 IPv4 位址

>
```

IPv4 正向對應區域查詢

34

檢測 DNS IPv4 A 設定(3/3)

- ```

> set type=ns // 指定查詢 NS 紀錄
> 80.201.210.in-addr.arpa // 輸入要查詢的網域
伺服器: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171

80.201.210.in-addr.arpa nameserver = ns1.w201201.ipv6lab.tw // 回應網域的 name server
ns1.w201201.ipv6lab.tw internet address = 210.201.80.171

```
- ```

> set type=ptr // 指定查詢 ptr 紀錄
> 210.201.80.171 // 輸入要查詢的 IPv4 位址
伺服器: ns1.w201201.ipv6lab.tw
Address: 210.201.80.171

172.80.201.210.in-addr.arpa name = www.w201201.ipv6lab.tw // 回應對應的第一筆資料
172.80.201.210.in-addr.arpa name = ns1.w201201.ipv6lab.tw // 回應對應的第二筆資料

```

詢

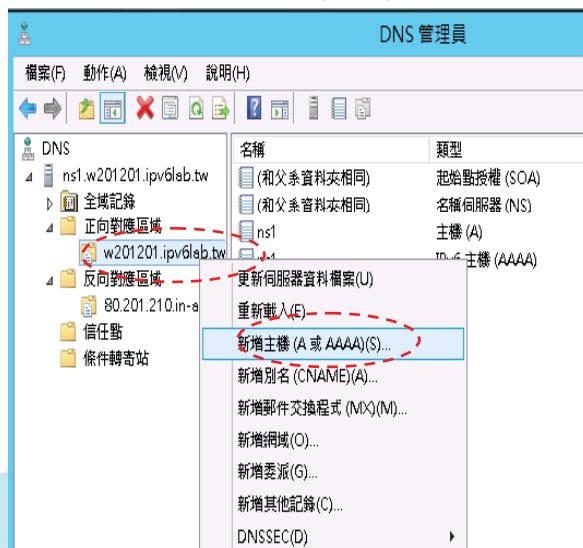
35

設定 DNS IPv6 AAAA 紀錄(1/8)

Windows 2012 預設啟用 IPv6 通訊協定，而且提供完整的 IPv4/IPv6 雙協定 DNS 管理圖形操作介面

- 設定 IPv6 主機正向對應紀錄(AAAA Record)

- 在 DNS 管理視窗點選『正向對應區域』，在『w201201.ipv6lab.tw』上點選滑鼠『右鍵』

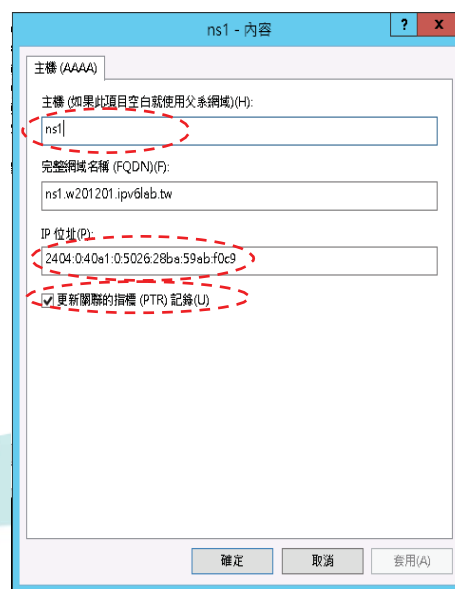


新增 AAAA 紀錄

36

設定 DNS IPv6 AAAA 紀錄(2/8)

- 先設定 DNS 主機的正向對應紀錄，所以在『名稱』輸入『ns1』，在『IP 位址』輸入『2404:0:40a1:0:5026:28ba:59ab:f0c9』，勾選『建立關聯的指標(PTR)紀錄』，自動建立反向解析→再按『新增主機』

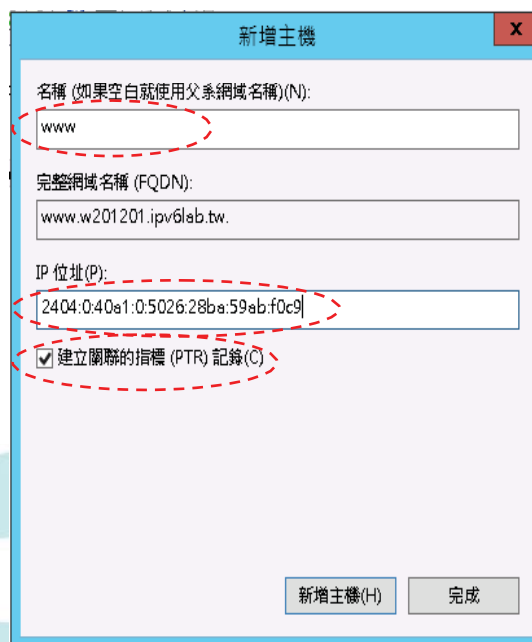


設定 DNS 主機正向對應紀錄

37

設定 DNS IPv6 AAAA 紀錄(3/8)

- 繼續設定 WWW 主機的正向對應紀錄，在『名稱』輸入『www』，在『IP 位址』輸入『2404:0:40a1:0:5026:28ba:59ab:f0c9』→勾選『建立關聯的指標(PTR)紀錄』，自動建立反向解析→再按『新增主機』



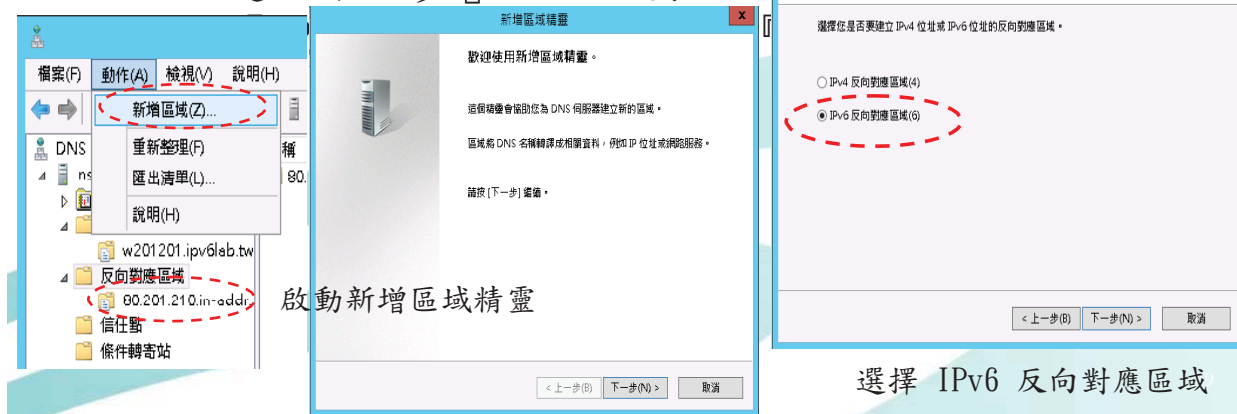
設定 WWW 主機正向對應紀錄

38

設定 DNS IPv6 AAAA 紀錄(4/8)

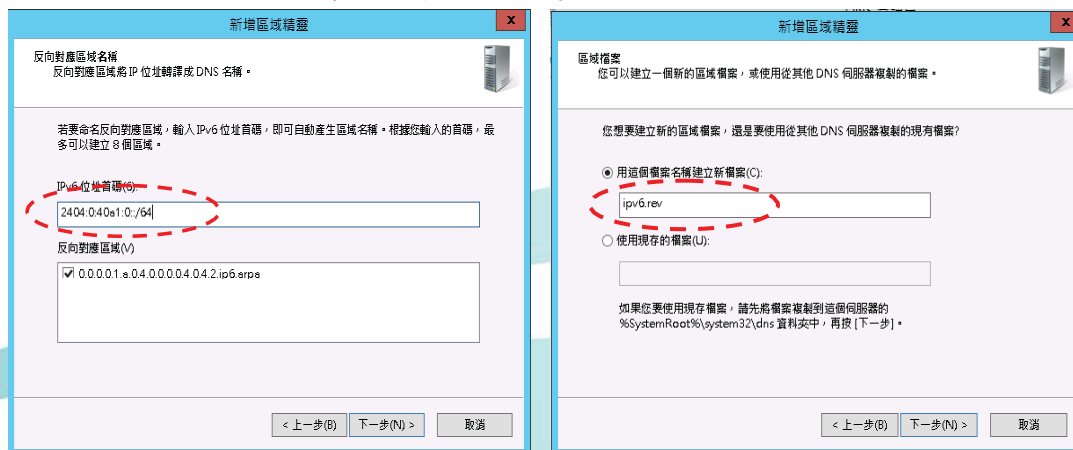
● 設定 IPv6 主機反向對應區域(IPv6 Reverse Zone)

- 從 DNS 的管理員左方視窗點選『反向對應區域』
→『新增區域』，啟動新增區域精靈
- 點選『下一步』→『主要區域』



設定 DNS IPv6 AAAA 紀錄(5/8)

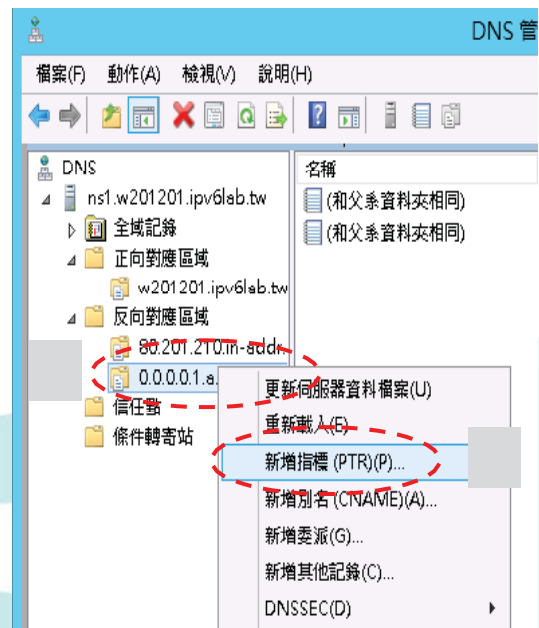
- 在『IPv6 位址首碼』輸入 IPv6 位址的位址首碼(Prefix)，本範例為2404:0:40a1:0::/64，請注意最後的 ” ::/64”。『反向對應區域』內的 資料會自動出現
- 『下一步』→區域檔案名稱：可自行設定檔名，本範例為『ipv6.rev』→動態更新：選擇『不允許動態更新』讓我們完全由手動新增 記錄在完成反向區域設定



設定 DNS IPv6 AAAA 紀錄(6/8)

- 設定主機 IPv6 反向對應紀錄(IPv6 PTR Record) 在建立反向對應區域後，新增正向對應紀錄時可同時自動建立反向對應紀錄，如果反向對應紀錄 PTR)沒有自動產生，則需要手動設定

- 在 DNS 管理視窗的 IPv6 反向對應區域『0.0.0.0.1.a.0.4.0.0.0.0.4.0.4.2.i p6.arpa』上點選滑鼠『右鍵』，選擇『新增指標(PTR)』

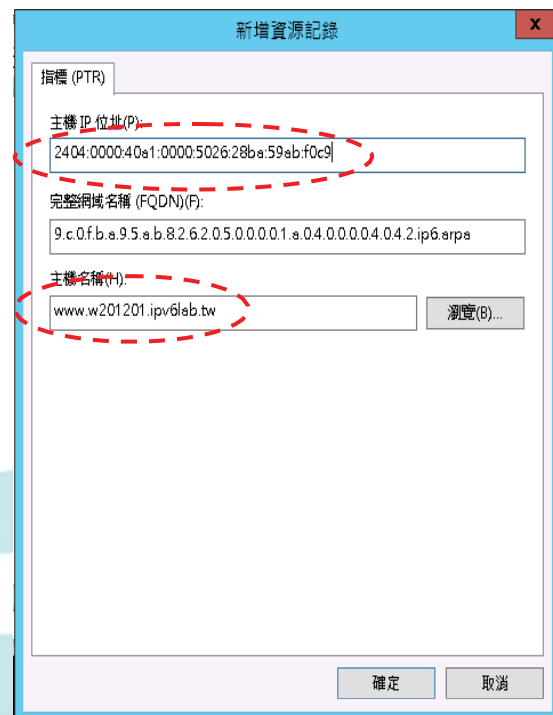


新增指標(PTR)

41

設定 DNS IPv6 AAAA 紀錄(7/8)

- 設定 DNS 主機反向對應紀錄，主機 IP 位址輸入『2404:0000:40a1:0000:5026:28ba:59ab:f0c9』(請注意，IPv6 位址不能使用簡寫，所有的 0 都要輸入)，主機名稱輸入『ns1.w201201.ipv6lab.tw』，

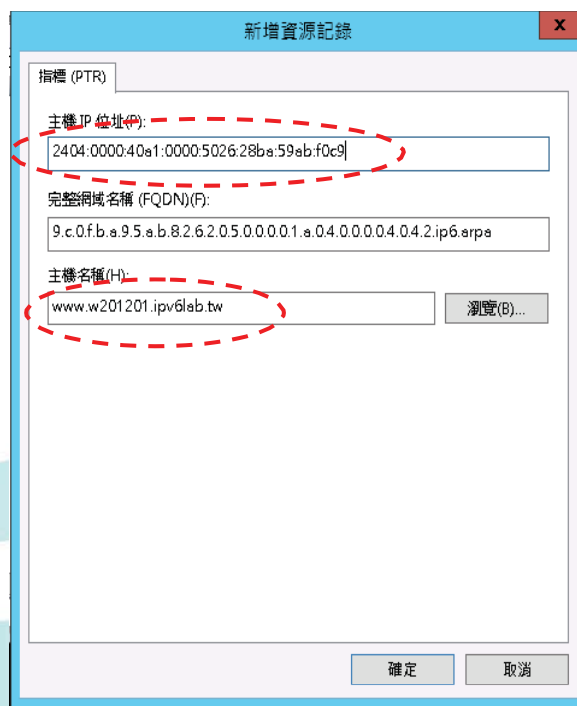


設定 DNS 主機反向對應紀錄

42

設定 DNS IPv6 AAAA 紀錄(8/8)

- 設定 WWW 主機反向對應紀錄，主機 IP 位址輸入『2404:0000:40a1:0000:5026:28ba:59ab:f0c9』，主機名稱輸入『www.w201201.ipv6lab.tw』



設定 WWW 主機反向對應紀錄

43

檢測 DNS IPv6 AAAA 設定(1/4)

利用 nslookup 指令檢查 DNS 設定是否正常，檢查方式請參考以下示範，操作過程出現 Non-existent domain 表示 DNS 找不到查詢的資料，請檢查 DNS 設定。

C:\Users\Administrator> nslookup // 使用 nslookup 命令查詢

預設伺服器: ns1.w201201.ipv6lab.tw
Address: 2404:0:40a1:0:5026:28ba:59ab:f0c9

> server ns1.w201201.ipv6lab.tw // 指定 DNS 查詢主機

預設伺服器: ns1.w201201.ipv6lab.tw
Addresses: 2404:0:40a1:0:5026:28ba:59ab:f0c9
210.201.80.171

44

檢測 DNS IPv6 AAAA 設定(2/4)

● IPv6 正向對應紀錄(A Record)查詢

<pre>> set type=aaaa // 指定查詢 A 紀錄 > ns1.w201201.ipv6lab.tw // 輸入要查詢的網址 伺服器: ns1.w201201.ipv6lab.tw Addresses: 2404:0:40a1:0:5026:28ba:59ab:f0c9 // 回應對應的 IPv6 位址 210.201.80.171 名稱: ns1.w201201.ipv6lab.tw Address: 2404:0:40a1:0:5026:28ba:59ab:f0c9 > www.w201201.ipv6lab.tw 伺服器: ns1.w201201.ipv6lab.tw Addresses: 2404:0:40a1:0:5026:28ba:59ab:f0c9 210.201.80.171 名稱: www.w201201.ipv6lab.tw Address: 2404:0:40a1:0:5026:28ba:59ab:f0c9 ></pre>	<pre>> set type=ns // 指定查詢 NS 紀錄 > 0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa // 輸入要查詢的網域 伺服器: ns1.w201201.ipv6lab.tw Addresses: 2404:0:40a1:0:5026:28ba:59ab:f0c9 210.201.80.171 0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa nameserver = ns1.w201201.ipv6lab.tw // 回應網域的 name server ns1.w201201.ipv6lab.tw internet address = 210.201.80.171 ns1.w201201.ipv6lab.tw AAAA IPv6 address = 2404:0:40a1:0:5026:28ba:59ab:f0c9 ></pre>
--	--

IPv6 正向對應區域查詢

IPv6 NS 紀錄查詢

45

檢測 DNS IPv6 AAAA 設定(3/4)

```
> set type=ptr // 指定查詢 ptr 紀錄
> 2404:0:40a1:0:5026:28ba:59ab:f0c9 // 輸入要查詢的 IPv6 位址
伺服器: ns1.w201201.ipv6lab.tw
Addresses: 2404:0:40a1:0:5026:28ba:59ab:f0c9
210.201.80.171

9.c.0.f.a.b.9.5.a.b.8.2.6.2.0.5.0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa name =
www.w201201.ipv6lab.tw // 回應對應的第一筆網址
9.c.0.f.a.b.9.5.a.b.8.2.6.2.0.5.0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa name =
ns1.w201201.ipv6lab.tw // 回應對應的第二筆網址

>
```

IPv6 反向對應區域查詢

46

檢測 DNS IPv6 AAAA 設定(4/4)

- 上層 DNS 的設定：

本範例 DNS 管理網域為 w201201.ipv6lab.tw，
上層隸屬於 ipv6lab.tw 網域，所以上層的
DNS 必須對 w201201.ipv6lab.tw 網域的 NS 記
錄、A 記錄及 AAAA 記錄進行授權。需請上

\$ORIGIN ipv6lab.tw.

lab2012 NS 管理單位增加的記錄如下：

ns1.lab2012 IN A 210.201.80.171

ns1.lab2012 IN AAAA 2404:0:40a1:0:5026:28ba:59ab:f0c9

47

Thank You

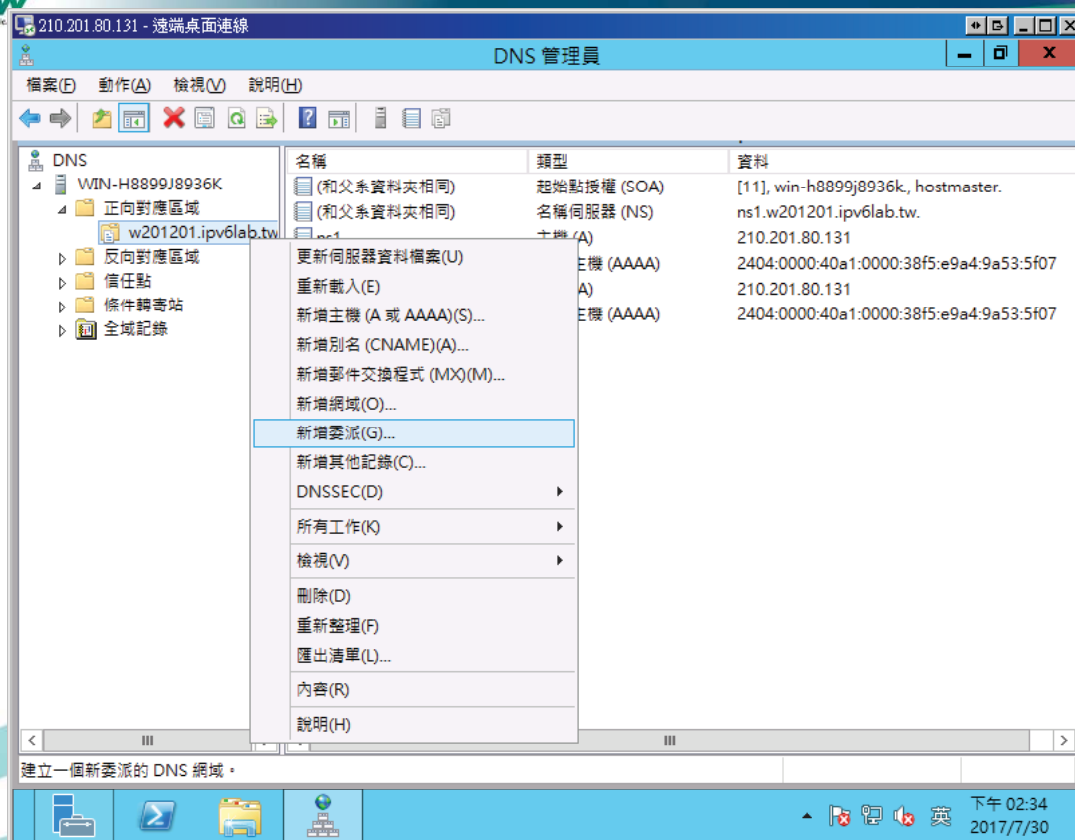


Windows Server 2012 DNS升級IPv6 新增委派DNS

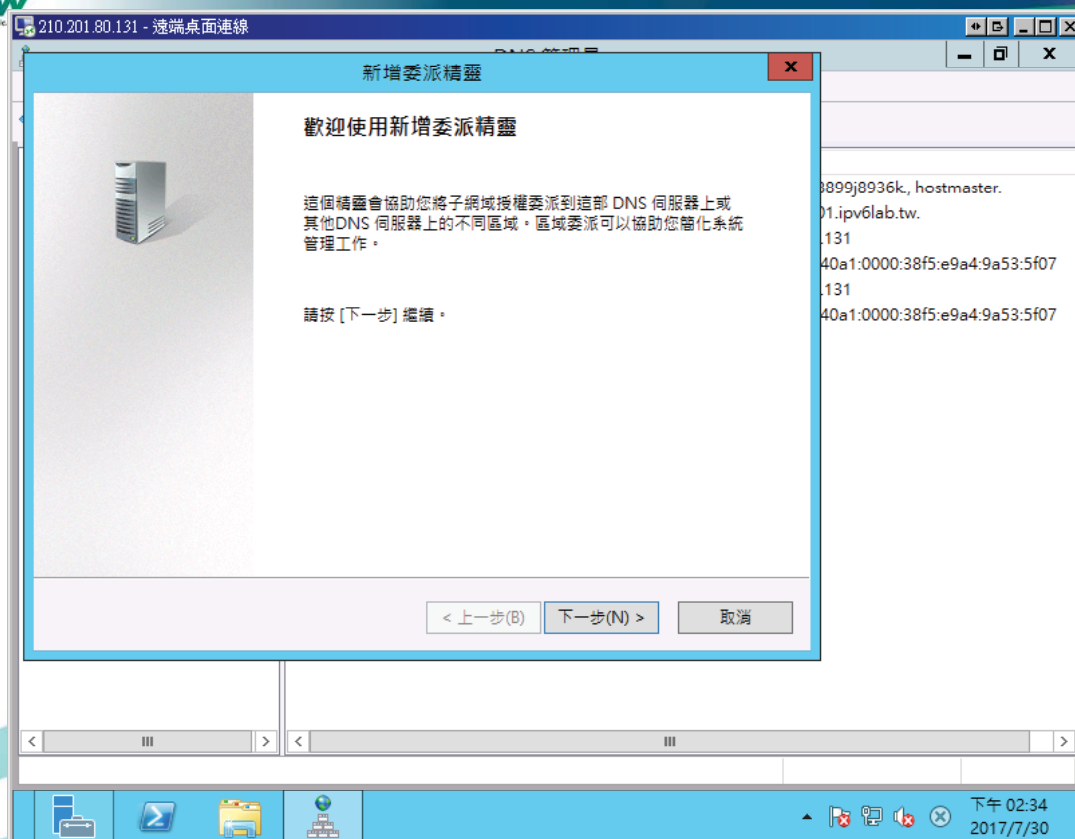


DNS設定相關資訊

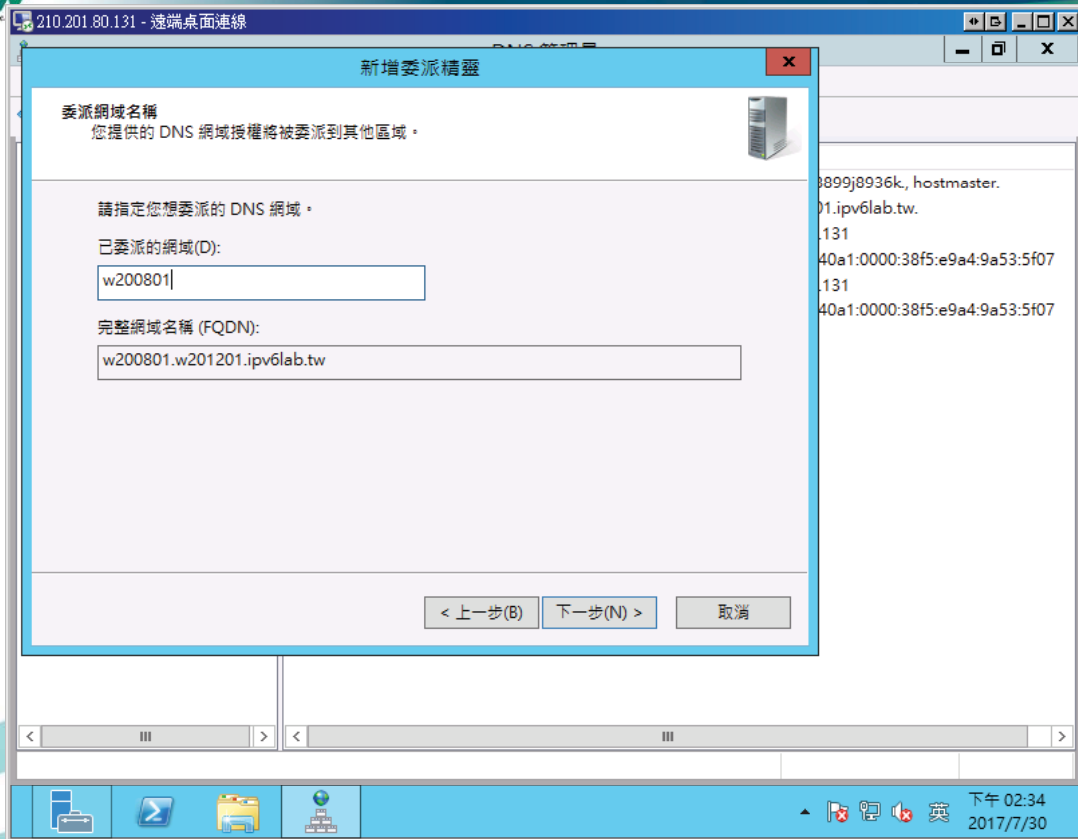
- 已設定DNS Server(Windows 2012)
 - 網域: w201201.ipv6lab.tw
 - DNS Server: ns1.w201201.ipv6lab.tw
 - IPv4: 210.201.80.131
 - IPv6: 2404:0:40a1:0:38f5:e9a4:9a53:5f07
- 新增委派DNS(Windows 2008)
 - 網域: w200801.w201201.ipv6lab.tw
 - DNS Server: ns1.w200801.w201201.ipv6lab.tw
 - IPv4: 210.201.80.41
 - IPv6: 2404:0:40a1:0:c881:5840:7150:4cbe



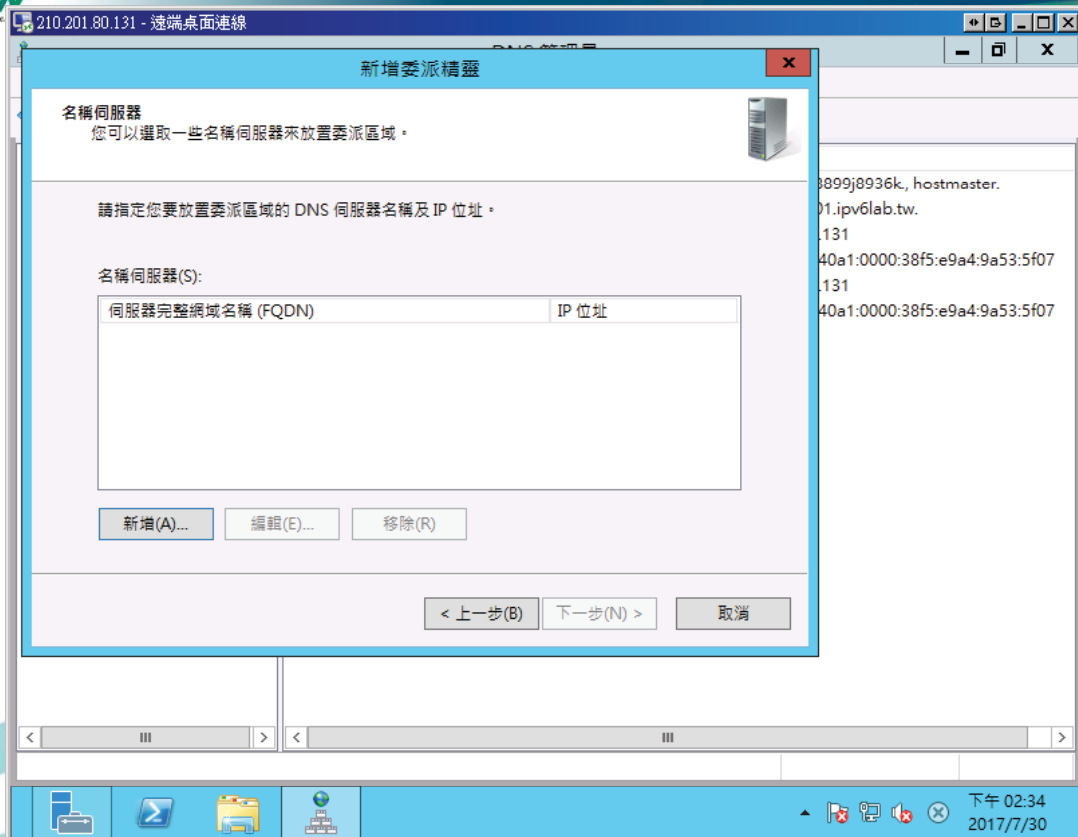
3



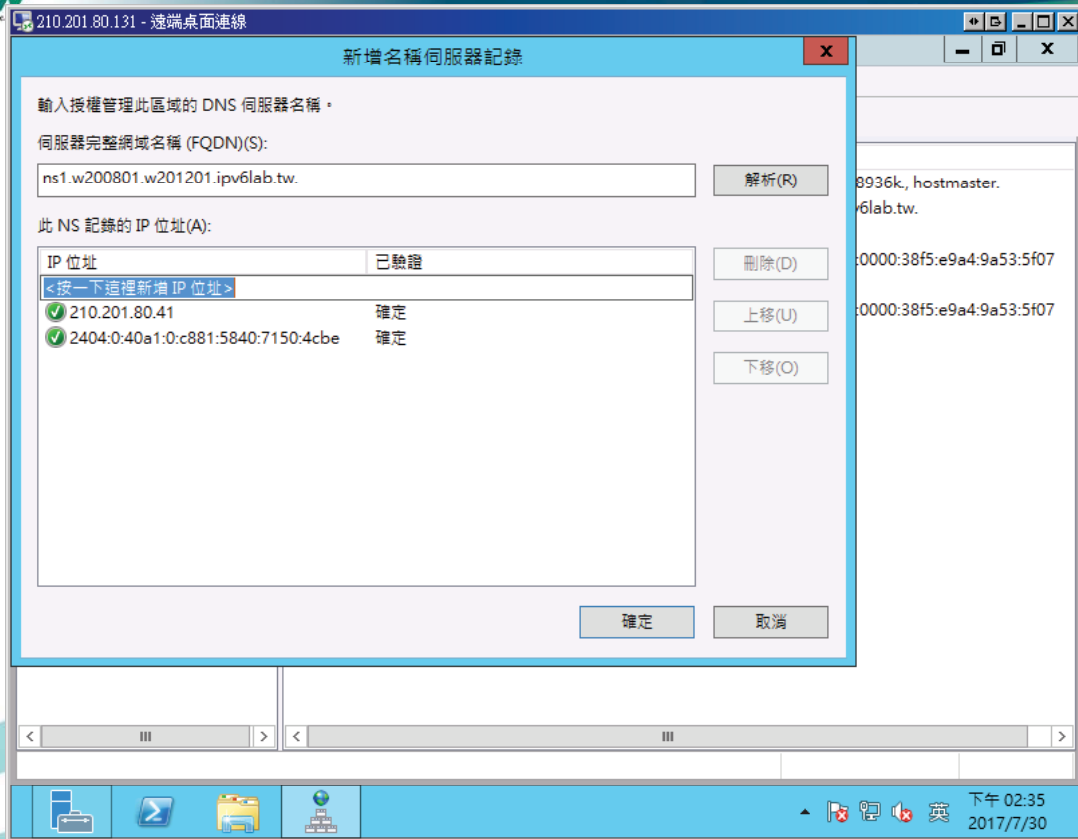
4



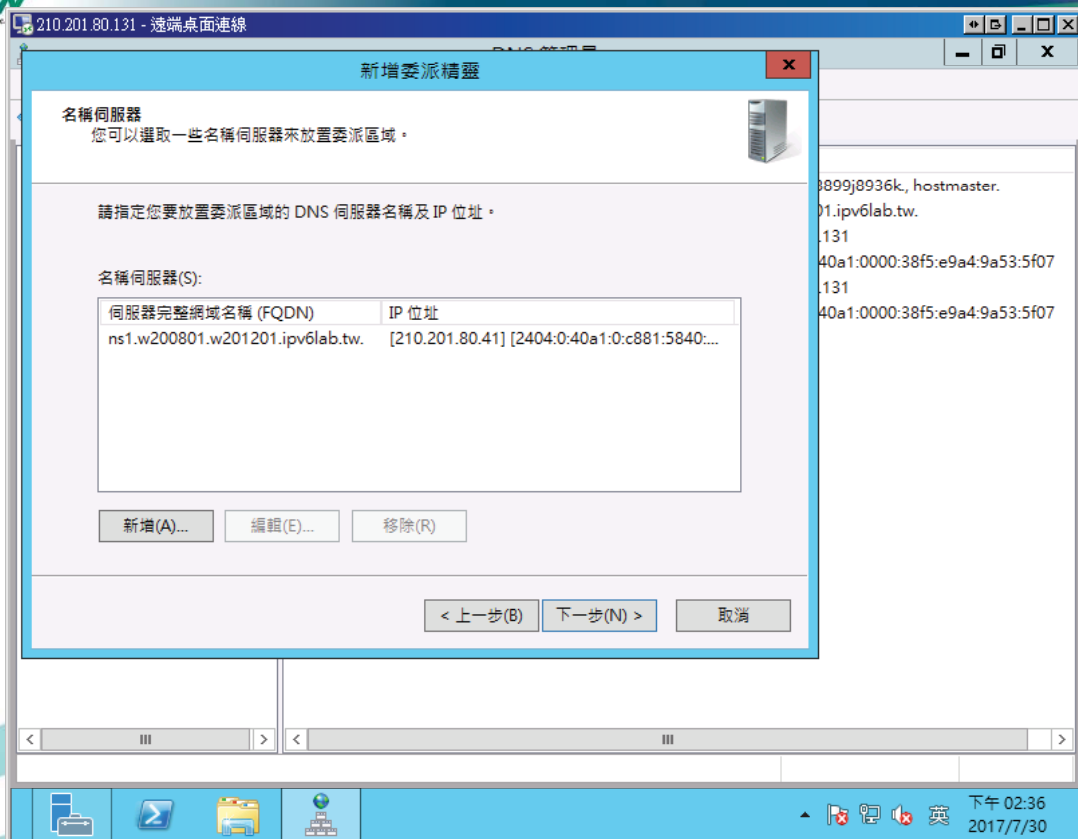
5



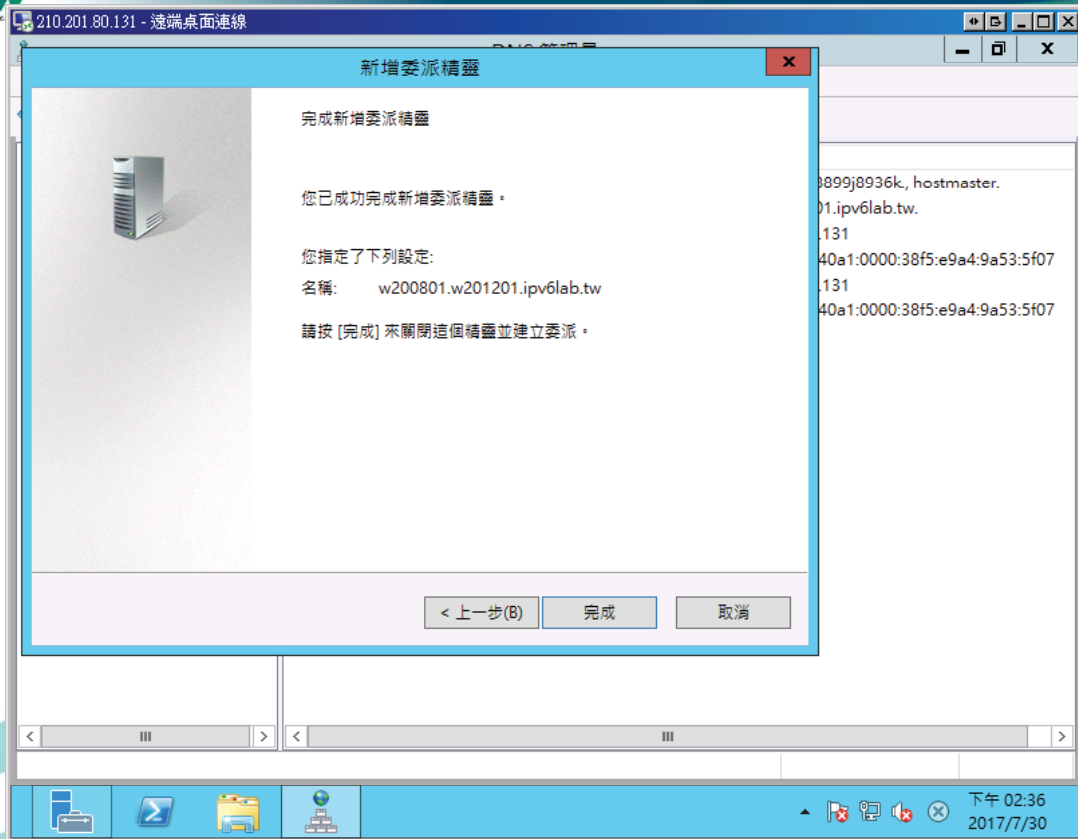
6



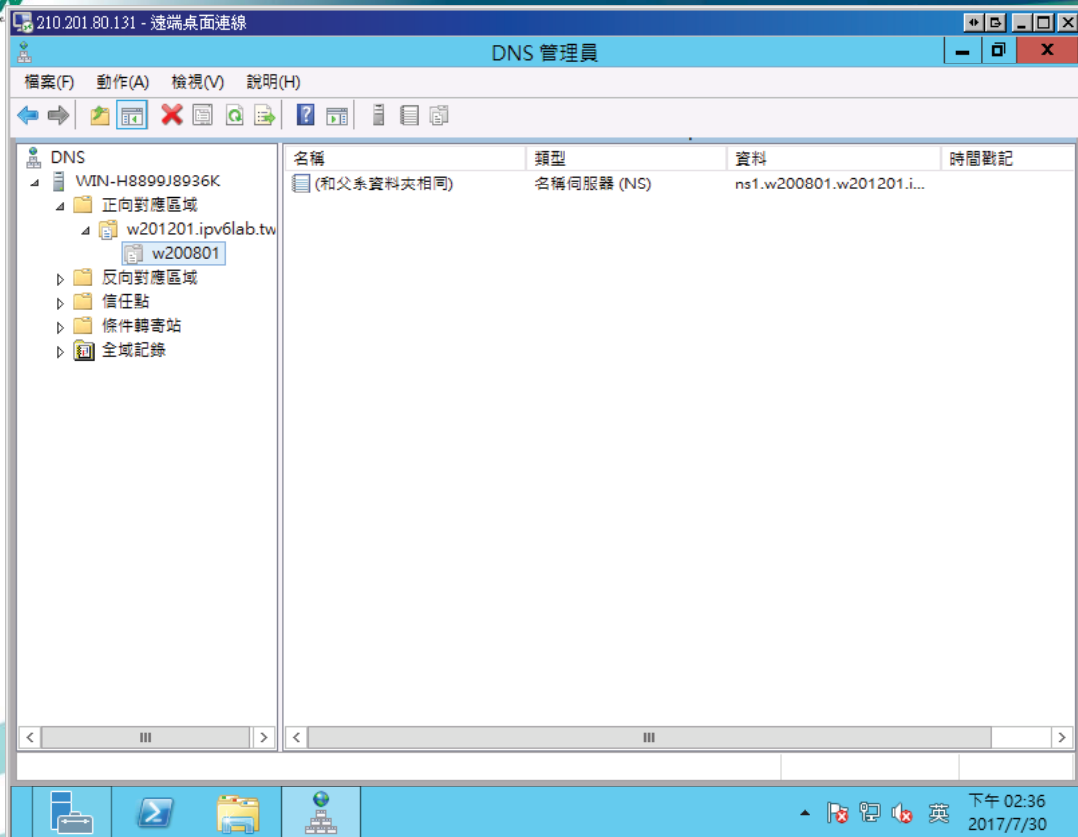
7



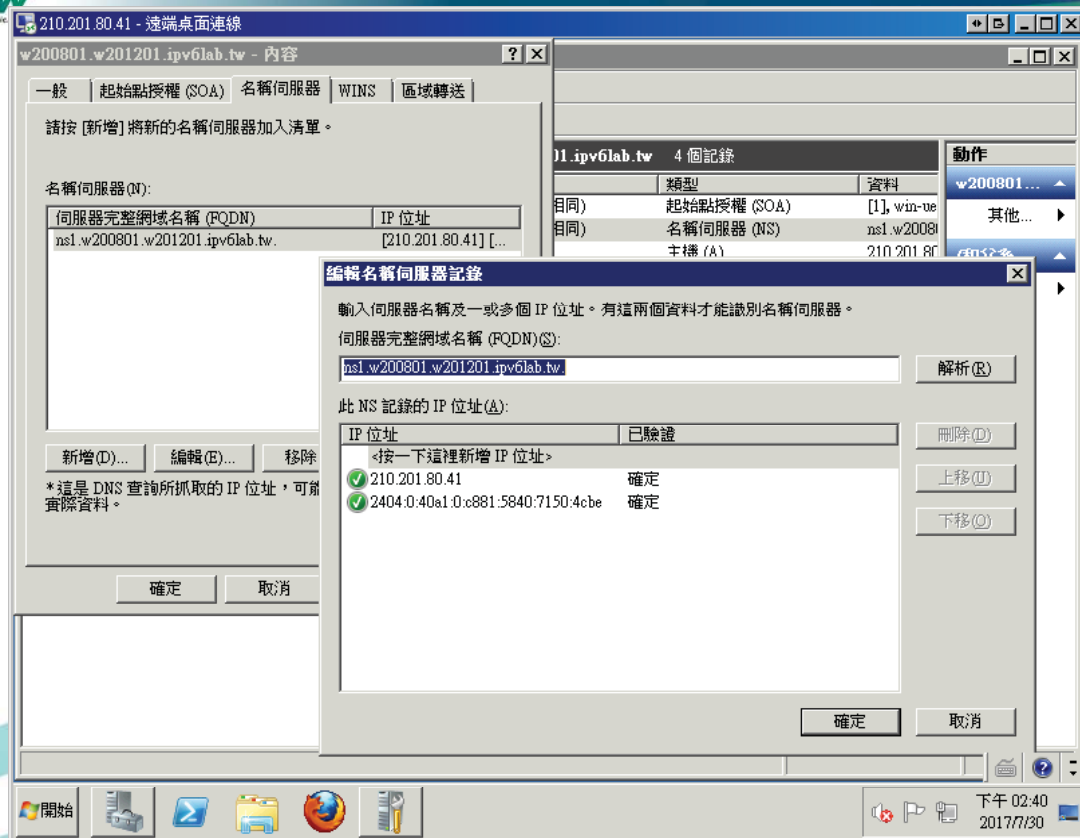
8



9



10



11

```

root@localhost:~
[ root@localhost ~]#
[ root@localhost ~]# dig ns1.w200801.w201201.ipv6lab.tw +trace aaaa

<<>> DiG 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12 <<>> ns1.w200801.w201201.ipv6lab.tw +trace aaaa
; global options: printcmd
1722 IN NS m.root-servers.net.
1722 IN NS k.root-servers.net.
1722 IN NS l.root-servers.net.
1722 IN NS j.root-servers.net.
1722 IN NS c.root-servers.net.
1722 IN NS i.root-servers.net.
1722 IN NS b.root-servers.net.
1722 IN NS g.root-servers.net.
1722 IN NS d.root-servers.net.
1722 IN NS e.root-servers.net.
1722 IN NS f.root-servers.net.
1722 IN NS h.root-servers.net.
1722 IN NS a.root-servers.net.
; Received 228 bytes from 168.95.1.1#53(168.95.1.1) in 3 ms

tw. 172800 IN NS sec4.apnic.net.
tw. 172800 IN NS h.dns.tw.
tw. 172800 IN NS c.dns.tw.
tw. 172800 IN NS b.dns.tw.
tw. 172800 IN NS e.dns.tw.
tw. 172800 IN NS ns.twnic.net.
tw. 172800 IN NS i.dns.tw.
tw. 172800 IN NS d.dns.tw.
tw. 172800 IN NS a.dns.tw.
tw. 172800 IN NS g.dns.tw.
tw. 172800 IN NS f.dns.tw.
; Received 507 bytes from 2001:dc3::35#53(m.root-servers.net) in 54 ms

ipv6lab.tw. 86400 IN NS ns1.ipv6day.tw.
ipv6lab.tw. 86400 IN NS ns2.ipv6day.tw.
; Received 180 bytes from 2001:dc0:4001:1:0:1836:0:141#53(sec4.apnic.net) in 205 ms

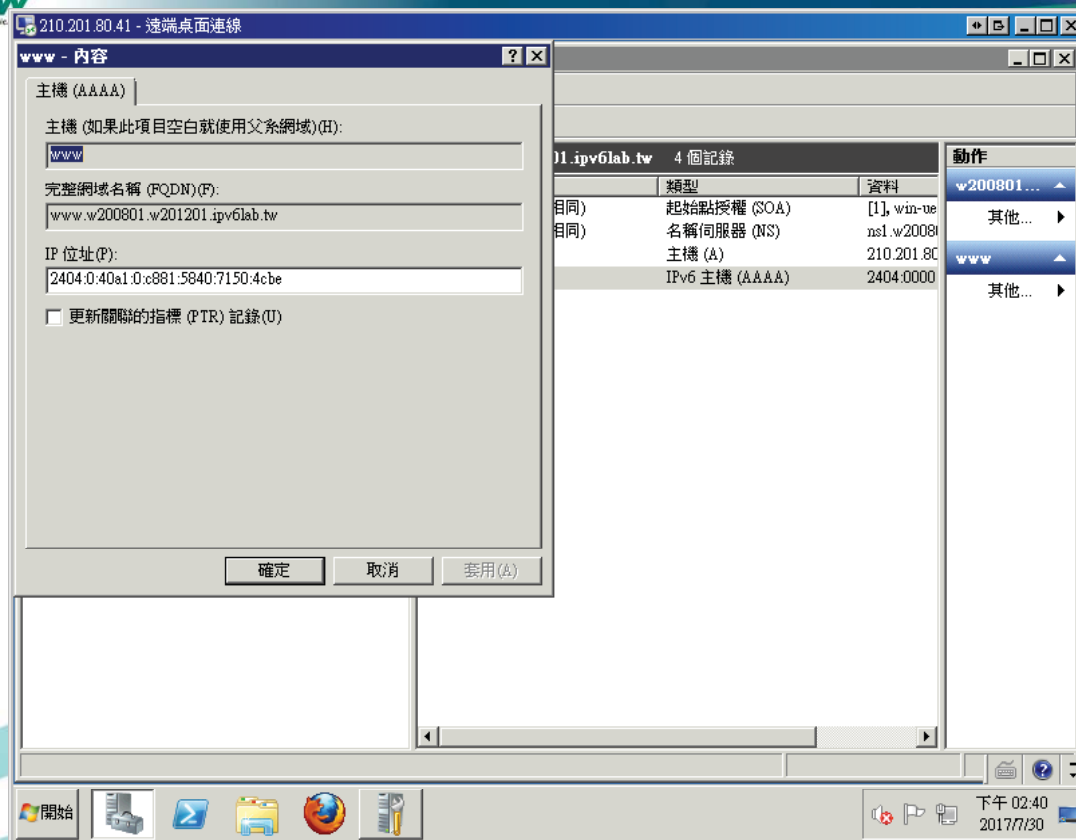
w201201.ipv6lab.tw. 60 IN NS ns1.w201201.ipv6lab.tw.
; Received 110 bytes from 2405:7e00:1002::199#53(ns1.ipv6day.tw) in 2 ms

w200801.w201201.ipv6lab.tw. 3600 IN NS ns1.w200801.w201201.ipv6lab.tw.
; Received 136 bytes from 2404:0:40a1:0:38f5:e9a4:9a53:5f07#53(ns1.w201201.ipv6lab.tw) in 0 ms

ns1.w200801.w201201.ipv6lab.tw. 3600 IN AAAA 2404:0:40a1:0:c881:5840:7150:4cbe
; Received 76 bytes from 2404:0:40a1:0:c881:5840:7150:4cbe#53(ns1.w200801.w201201.ipv6lab.tw) in 15 ms

[ root@localhost ~]#

```



13

```

root@localhost:~
[ root@localhost ~ ]#
[ root@localhost ~ ]# dig www.w200801.w201201.ipv6lab.tw +trace aaaa

;<>> DiG 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12 <>> www.w200801.w201201.ipv6lab.tw +trace aaaa
; global options: printcmd
71076 IN NS g.root-servers.net.
71076 IN NS i.root-servers.net.
71076 IN NS k.root-servers.net.
71076 IN NS d.root-servers.net.
71076 IN NS b.root-servers.net.
71076 IN NS m.root-servers.net.
71076 IN NS e.root-servers.net.
71076 IN NS h.root-servers.net.
71076 IN NS c.root-servers.net.
71076 IN NS j.root-servers.net.
71076 IN NS f.root-servers.net.
71076 IN NS a.root-servers.net.
; Received 228 bytes from 168.95.1.1#53(168.95.1.1) in 3 ms

tw. 172800 IN NS ns.twmic.net.
tw. 172800 IN NS c.dns.tw.
tw. 172800 IN NS a.dns.tw.
tw. 172800 IN NS e.dns.tw.
tw. 172800 IN NS h.dns.tw.
tw. 172800 IN NS f.dns.tw.
tw. 172800 IN NS b.dns.tw.
tw. 172800 IN NS i.dns.tw.
tw. 172800 IN NS g.dns.tw.
tw. 172800 IN NS d.dns.tw.
tw. 172800 IN NS sec4.apnic.net.
; Received 507 bytes from 2001:500:12::d0d#53(g.root-servers.net) in 245 ms

ipv6lab.tw. 86400 IN NS ns1.ipv6day.tw.
ipv6lab.tw. 86400 IN NS ns2.ipv6day.tw.
; Received 180 bytes from 2001:288:1:1006::11#53(ns.twmic.net) in 2 ms

w201201.ipv6lab.tw. 60 IN NS ns1.w201201.ipv6lab.tw.
; Received 110 bytes from 2405:7e00:1002::199#53(ns1.ipv6day.tw) in 2 ms

w200801.w201201.ipv6lab.tw. 3600 IN NS ns1.w200801.w201201.ipv6lab.tw.
; Received 136 bytes from 2404:0:40a1:0:c881:5840:7150:4cbe#53(ns1.w201201.ipv6lab.tw) in 3 ms

www.w200801.w201201.ipv6lab.tw. 3600 IN AAAA 2404:0:40a1:0:c881:5840:7150:4cbe
; Received 76 bytes from 2404:0:40a1:0:c881:5840:7150:4cbe#53(ns1.w200801.w201201.ipv6lab.tw) in 2 ms

[ root@localhost ~ ]#

```

Thank You





Linux Server升級 至IPv6



大綱

- Linux的IPv6設定
 - ▣ DNS Server(Bind)的IPv6設定
 - ▣ WEB Server(Apache)的IPv6設定

Linux的IPv6設定

- Linux Kernel 在 2.1.8 即加入IPv6的部份功能，現今的Linux Kernel 2.6.x 中，IPv6已經是被完整地支援。在2008年12月1日，Linux Foundation(Linux基金會)宣佈IPv6在Linux主要的Distribution(發行版)中已經相容美國國防部的標準(連結)。
- 現在只要下載任何一個常見的Distribution，都可以支援IPv6。本文件教學以 CentOS 5.x 作為示範的作業系統。

Linux的IPv6設定

- 圖型視窗設定
 - CentOS在安裝時，系統已經預設啟動IPv6功能，使用者可在圖形界面視窗中進行手動設定IPv6位址



Linux的IPv6設定

- 網路組態檔案設定

- ① 開啟IPv6網路介面

編輯 **/etc/sysconfig/network**，加入：

NETWORKING_IPV6=yes

- ② 設定IPv6位址及Gateway

編輯 **/etc/sysconfig/network-scripts/ifcfg-eth0**，加入

IPV6INIT=yes

IPV6ADDR=<IPv6-IP-Address>

IPV6_DEFAULTGW=<IPv6-IP-Gateway-Address>

- ③ 重新啟動網路

service network restart

```
[root@localhost ~]# /etc/init.d/network restart
Shutting down interface eth0: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0:
Determining IP information for eth0... done. [ OK ]
[root@localhost ~]#
```

驗證IPv6通訊協定

- 驗證啟動IPv6通訊協定

- Command : **ping6 ::1**

```
[root@labcentosad]# ping6 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=0 ttl=64 time=0.019 ms
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.020 ms
--- ::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.019/0.021/0.025/0.006 ms, pipe 2
[root@labcentosa]#
```

驗證IPv6通訊協定

- 驗證IPv6位址

- Command : # **/sbin/ifconfig**

```
[root@localhost ~]# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5D:50:F3:7B
          inet addr:210.201.80.1  Bcast:210.201.80.255  Mask:255.255.255.0
          inet6 addr: 2404:0:40a1:0:215:5dff:fe50:f37b/64 Scope:Global
          inet6 addr: fe80::215:5dff:fe50:f37b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:211195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17742624 (16.9 MiB)  TX bytes:7359192 (7.0 MiB)
[root@localhost ~]#
```

驗證IPv6通訊協定

- 驗證對外IPv6連線

- Command : **ping6 www.ipv6.org.tw**

```
[root@labcentosad]# ping6 www.ipv6.org.tw
PING www.ipv6.org.tw(2001:c50:ffff:1:21a:92ff:fe43:d665) 56 data bytes
64 bytes from 2001:c50:ffff:1:21a:92ff:fe43:d665: icmp_seq=0 ttl=53 time=102 ms
64 bytes from 2001:c50:ffff:1:21a:92ff:fe43:d665: icmp_seq=1 ttl=53 time=10.5 ms
64 bytes from 2001:c50:ffff:1:21a:92ff:fe43:d665: icmp_seq=2 ttl=53 time=29.0 ms
64 bytes from 2001:c50:ffff:1:21a:92ff:fe43:d665: icmp_seq=3 ttl=53 time=35.7 ms
--- www.ipv6.org.tw ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 10.582/44.561/102.910/34.922 ms, pipe 2
[root@labcentosa]#
```

DNS SERVER (BIND)

9

更新yum套件

```
mkdir -p /var/cache/yum/base/  
mkdir -p /var/cache/yum/extras/  
mkdir -p /var/cache/yum/updates/  
  
echo "http://vault.centos.org/5.11/os/i386/" > /var/cache/yum/base/mirrorlist.txt  
echo "http://vault.centos.org/5.11/extras/i386/" > /var/cache/yum/extras/mirrorlist.txt  
echo "http://vault.centos.org/5.11/updates/i386/" > /var/cache/yum/updates/mirrorlist.txt
```

Bind 安裝

- 透過 yum 安裝 Bind 與其設定檔範本
 - #yum -y install bind system-config-bind bind-chroot

```
[root@localhost ~]# yum -y install bind system-config-bind bind-chroot
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: ftp.isu.edu.tw
* updates: ftp.isu.edu.tw
* extras: ftp.isu.edu.tw
Setting up Install Process
Parsing package install arguments
-----<以下省略>-----
[root@localhost ~]#
```

Bind 設定檔

- 設定檔位置：/var/named/chroot/
 - 由於安全性考量，安裝完 bind-chroot 套件後，bind 的設定檔位置會改到 /var/named/chroot 下
 - system-config-bind 套件則是安裝bind預設的設定檔，位置在
/usr/share/system-config-bind/profiles/default 下
- 設定檔放置步驟
 - ① named.conf
 - 先到 /usr/share/system-config-bind/profiles/default 將 named.conf 複製到 /var/named/chroot/etc
 - # **cd /usr/share/system-config-bind/profiles/default/**
 - # **cp named.conf /var/named/chroot/etc/**

Bind 設定檔

② 正反解檔案

- 到 /usr/share/system-config-bind/profiles/default/named 去複製系統預設的正反解檔案(zone)
- # **cd /usr/share/system-config-bind/profiles/default/named**
- # **cp *.* /var/named/chroot/var/named/**

```
[root@localhost ~]# cd /usr/share/system-config-bind/profiles/default/named
[root@localhost ~]# ls
localdomain.zone  localhost.zone  named.broadcast  named.ip6.local  named.local
named.zero
[root@localhost ~]# cp *.* /var/named/chroot/var/named/
[root@localhost ~]#
```

Bind 設定檔

③ 複製ROOT伺服器位址設定檔案

- 到 /usr/share/doc/bind-9.3.6/sample/var/named 複製 named.root 到 /var/named/chroot/var/named/
- # **cd /usr/share/doc/bind-9.3.6/sample/var/named**
- # **cp named.root /var/named/chroot/var/named/**

● 啟動 bind

- **/etc/init.d/named start**

```
[root@localhost ~]# /etc/init.d/named start
Starting named:
[root@localhost ~]#
```

[OK]

使用參考設定檔

```

root@localhost:~# wget http://lab2.v6lab.tw/directory/ipv6labahyperv/ipv6lab_named_cent01.ipv6lab.tw.zip -O /root/named.zip
--2017-07-23 12:24:43-- http://lab2.v6lab.tw/directory/ipv6labahyperv/ipv6lab_named_cent01.ipv6lab.tw.zip
Resolving lab2.v6lab.tw... 210.201.80.128, 2404:0:40a1::128
Connecting to lab2.v6lab.tw|210.201.80.128|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5430 (5.3K) [application/zip]
Saving to: '/root/named.zip'

100%[=====>] 5,430      34.6K/s  in 0.2s

2017-07-23 12:24:44 (34.6 KB/s) - '/root/named.zip' saved [5430/5430]

[root@localhost ~]# cd /
[root@localhost /]#
[root@localhost /]# unzip -u /root/named.zip
Archive: /root/named.zip
  creating: var/named/
  creating: var/named/chroot/
  creating: var/named/chroot/etc/
  inflating: var/named/chroot/etc/named.conf
  extracting: var/named/chroot/etc/rndc.key
  creating: var/named/chroot/var/
  creating: var/named/chroot/var/named/
  inflating: var/named/chroot/var/named/0.0.0.1.a.0.4.0.0.0.4.0.4.2.rev
  inflating: var/named/chroot/var/named/cent01.ipv6lab.tw.zone
  inflating: var/named/chroot/var/named/localdomain.zone
  inflating: var/named/chroot/var/named/localhost.zone
  inflating: var/named/chroot/var/named/name.ipv6lab.rev
  inflating: var/named/chroot/var/named/named.broadcast
  inflating: var/named/chroot/var/named/named.ip6.local
  inflating: var/named/chroot/var/named/named.local
  inflating: var/named/chroot/var/named/named.root
  inflating: var/named/chroot/var/named/named.zero
[root@localhost /]#
[root@localhost /]#

```

啟用DNS服務

- 利用netstat 檢查 Bind 是否同時監聽 IPv4 與 IPv6 的 53 port
 - ❑ # **netstat -utlnp | grep named**
 - ❑ 可以看到已經在IPv4上啟用服務(但IPv6還未啟用)

```

[root@localhost ~]# netstat -utlnp | grep named
tcp        0      0 210.201.80.1:53      0.0.0.0:*             LISTEN      22786/named
tcp        0      0 127.0.0.1:53         0.0.0.0:*             LISTEN      22786/named
tcp        0      0 127.0.0.1:953       0.0.0.0:*             LISTEN      22786/named
tcp        0      0 :::1:953            :::*                   LISTEN      22786/named
udp        0      0 210.201.80.1:53      0.0.0.0:*             22786/named
udp        0      0 127.0.0.1:53        0.0.0.0:*             22786/named
[root@localhost ~]#

```

設定啟用IPv6 DNS服務

- 設定主設定檔

- 編輯/var/named/chroot/etc/named.conf

- 設定Options區塊資料，增加一行，儲存後，重新啟動named
 - # **vim /var/named/chroot/etc/named.conf**
 - # **/etc/init.d/named restart**

```
[root@localhost ~]# vim /var/named/chroot/etc/named.conf
options {
directory "/var/named";                //DNS資料預設放置的位置
dump-file "/var/named/data/cache_dump.db"; //一些統計資料存放路徑
statistics-file "/var/named/data/named_stats.txt"; //統計資料存放路徑
listen-on-v6 port 53 { any; };        //設定IPv6監聽的port
};
```

其他設定視需要調整

- 設定主設定檔

- 編輯/var/named/chroot/etc/named.conf

- 設定Options區塊資料

```
[root@localhost ~]# vim /var/named/chroot/etc/named.conf
options {
directory "/var/named";                //DNS資料預設放置的位置
dump-file "/var/named/data/cache_dump.db"; //一些統計資料存放路徑
statistics-file "/var/named/data/named_stats.txt"; //統計資料存放路徑
memstatistics-file "/var/named/data/named_mem_stats.txt";
listen-on port 53 { any; };            //設定監聽的port
listen-on-v6 port 53 { any; };        //設定IPv6監聽的port
allow-query { any; };                  //限制此台DNS 的使用者
allow-transfer { none; };              //設定Slave DNS
version "None of your business";       //隱藏DNS版號
forward only;
forwarders { 168.95.1.1;
168.95.192.2; };                      //DNS伺服器無法解析時，會交由其他台DNS解析
};
```

設定正解設定檔

□ 設定zone區塊正解資料

```
[root@localhost ~]# vim /var/named/chroot/etc/named.conf

zone "cent01.ipv6lab.tw" IN {                                //正解zone file
    type master;                                           //本主機為master DNS
    file "cent01.ipv6lab.tw.zone";                         //正解zone file檔案名稱
    allow-update { none; };                                //不允許動態更新服務
};
```

設定IPv6正解內容

□ 進行IPv6正解設定

- 編輯/var/named/chroot/var/named/cent01.ipv6lab.tw.zone
- # **vim /var/named/chroot/var/named/cent01.ipv6lab.tw.zone**

```
$TTL      86400
$ORIGIN cent01.ipv6lab.tw.
@         IN SOA      @ hostmaster.cent01.ipv6lab.tw. (
                                20130709      ; serial
                                3H             ; refresh
                                15M            ; retry
                                1W             ; expiry
                                1D )           ; minimum
@         IN NS       ns1.cent01.ipv6lab.tw.
ns1       IN AAAA     2404:0:40a1:0:215:5dff:fe50:f37b
ns1       IN A        210.201.80.1
www       IN A        210.201.80.1
www       IN AAAA     2404:0:40a1:0:215:5dff:fe50:f37b
```

設定反解設定檔

□ 設定zone區塊反解資料

```
[root@localhost ~]# vim /var/named/chroot/etc/named.conf

zone "80.201.210.in-addr.arpa." IN { //反解zone file
type master; //本主機為master DNS
file "name.ipv6lab.rev"; //反解檔案名稱
allow-update { none; }; //不允許動態更新服務
};

zone "0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa." IN {
//設定IPv6反解zone file
type master; //本主機為master DNS
file "0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.rev"; //反解檔案名稱
allow-update { none; }; //不允許動態更新服務
};
```

設定IPv4反解內容

● 進行IPv6反解(PTR)設定

- 編輯反解zone檔案
- # **vim /var/named/chroot/var/named/name.ipv6lab.rev**

```
$TTL      86400
@         IN      SOA      @      hostmaster.cent01.ipv6lab.tw. (
                                20130709      ; Serial
                                28800          ; Refresh
                                14400          ; Retry
                                3600000        ; Expire
                                86400 )        ; Minimum
@         IN      NS       ns1.cent01.ipv6lab.tw.
$ORIGIN 80.201.210.in-addr.arpa.
1         IN      PTR      ns1.cent01.ipv6lab.tw.
1         IN      PTR      www.cent01.ipv6lab.tw.
```

設定IPv6反解內容

- 進行IPv6反解(PTR)設定

- 編輯反解zone檔案

- # **vim /var/named/chroot/var/named/0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.rev**

```
$TTL      86400
@         IN      SOA      @         hostmaster.cent01.ipv6lab.tw. (
                                20130709    ; Serial
                                28800        ; Refresh
                                14400        ; Retry
                                3600000     ; Expire
                                86400 )     ; Minimum
@         IN      NS       ns1.cent01.ipv6lab.tw.
$ORIGIN 0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa.
b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0 IN PTR ns1.cent01.ipv6lab.tw.
b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0 IN PTR www.cent01.ipv6lab.tw.
```

設定完成，重新啟動Bind

- 重新啟動 Bind

- **/etc/init.d/named restart**

```
[root@localhost ~]# /etc/init.d/named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@localhost ~]#
```


IPv6 防火牆-ip6tables

- 進行IPv6防火牆設定
 - 編輯ip6tables檔案，加入以下2行
 - # **vim /etc/sysconfig/ip6tables**
 - 編輯完成後，重新啟動IPv6防火牆
 - # **/etc/init.d/ip6tables restart**

```
[root@localhost ~]# vim /etc/sysconfig/ip6tables
-----<以上省略>-----
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m udp -p udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
-----<以下省略>-----
[root@localhost ~]# /etc/init.d/ip6tables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading ip6tables modules: [ OK ]
Applying ip6tables firewall rules: [ OK ]
[root@localhost named]#
```

IPv4 防火牆-iptables

- 進行IPv4防火牆設定
 - 編輯iptables檔案，加入以下2行
 - # **vim /etc/sysconfig/iptables**
 - 編輯完成後，重新啟動IPv4防火牆
 - # **/etc/init.d/iptables restart**

```
[root@localhost ~]# vim /etc/sysconfig/iptables
-----<以上省略>-----
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m udp -p udp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
-----<以下省略>-----
[root@localhost ~]# /etc/init.d/iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
[root@localhost named]#
```

檢測IPv6正解

□ 檢查IPv6正解

```
[root@localhost ~]# nslookup
> server ns1.cent01.ipv6lab.tw
Default server: ns1.cent01.ipv6lab.tw
Address: 2404:0:40a1:0:215:5dff:fe50:f37b#53
Default server: ns1.cent01.ipv6lab.tw
Address: 210.201.80.1#53
> set type=aaaa
> ns1.cent01.ipv6lab.tw
Server:          ns1.cent01.ipv6lab.tw
Address:         2404:0:40a1:0:215:5dff:fe50:f37b#53

ns1.cent01.ipv6lab.tw      has AAAA address 2404:0:40a1:0:215:5dff:fe50:f37b
> www.cent01.ipv6lab.tw
Server:          ns1.cent01.ipv6lab.tw
Address:         2404:0:40a1:0:215:5dff:fe50:f37b#53

www.cent01.ipv6lab.tw     has AAAA address 2404:0:40a1:0:215:5dff:fe50:f37b
```

檢測IPv6反解

□ 檢查IPv6反解

```
[root@localhost ~]# nslookup
> server ns1.cent01.ipv6lab.tw
Default server: ns1.cent01.ipv6lab.tw
Address: 2404:0:40a1:0:215:5dff:fe50:f37b#53
Default server: ns1.cent01.ipv6lab.tw
Address: 210.201.80.1#53
> set type=ptr
> 2404:0:40a1:0:215:5dff:fe50:f37b
Server:          ns1.cent01.ipv6lab.tw
Address:         2404:0:40a1:0:215:5dff:fe50:f37b#53

b. 7. 3. f. 0. 5. e. f. f. f. d. 5. 5. 1. 2. 0. 0. 0. 0. 0. 1. a. 0. 4. 0. 0. 0. 0. 4. 0. 4. 2. ip6. arpa.
name = ns1.cent01.ipv6lab.tw.
name = www.cent01.ipv6lab.tw.
```

DNS檢測工具dig介紹

- dig - DNS lookup utility
 - 常用 dig debug 的幾個參數說明
 - -t type :指定query type , 如a, aaaa
 - -4:指定只透過 IPv4 進行查詢
 - -6:指定只透過 IPv6 進行查詢
 - +trace: 從最上層 dns root 往下逐步查詢並顯示詳細過程
 - @global-server: 指定使用哪台 cache DNS server
 - +short: 簡短輸出 (寫程式 追蹤方便使用)
 - -x: 反向查詢

檢測IPv6正解

- 使用dig只透過IPv6檢查IPv6 AAAA正解
- **dig www.cent01.ipv6lab.tw -t aaaa -6 +trace @2404:0:40a1:0:215:5dff:fe50:f37b**

```
[root@localhost ~]# dig www.cent01.ipv6lab.tw -t aaaa -6 +trace @2404:0:40a1:0:215:5dff:fe50:f37b

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6 <<>> www.cent01.ipv6lab.tw -t aaaa -6 +trace @2404:0:40a1:0:215:5dff:fe50:f37b
;; global options: printcmd
.                517537 IN      NS      d.root-servers.net.
.                517537 IN      NS      e.root-servers.net.
.                517537 IN      NS      f.root-servers.net.
.                517537 IN      NS      g.root-servers.net.
.                517537 IN      NS      h.root-servers.net.
.                517537 IN      NS      i.root-servers.net.
.                517537 IN      NS      j.root-servers.net.
.                517537 IN      NS      k.root-servers.net.
.                517537 IN      NS      l.root-servers.net.
.                517537 IN      NS      m.root-servers.net.
.                517537 IN      NS      a.root-servers.net.
.                517537 IN      NS      b.root-servers.net.
.                517537 IN      NS      c.root-servers.net.
;; Received 512 bytes from 2404:0:40a1:0:215:5dff:fe50:f37b#53 (2404:0:40a1:0:215:5dff:fe50:f37b) in 2 ms

tw.              172800 IN      NS      h.dns.tw.
tw.              172800 IN      NS      d.dns.tw.
tw.              172800 IN      NS      ns.twnic.net.
tw.              172800 IN      NS      e.dns.tw.
tw.              172800 IN      NS      c.dns.tw.
tw.              172800 IN      NS      b.dns.tw.
tw.              172800 IN      NS      f.dns.tw.
tw.              172800 IN      NS      sec4.apnic.net.
tw.              172800 IN      NS      g.dns.tw.
tw.              172800 IN      NS      a.dns.tw.
;; Received 494 bytes from 2001:500:2d::d#53(d.root-servers.net) in 33 ms

ipv6lab.tw.      86400 IN      NS      ns1.ipv6day.tw.
ipv6lab.tw.      86400 IN      NS      ns2.ipv6day.tw.
;; Received 171 bytes from 2405:7e00:1001::11#53(h.dns.tw) in 18 ms

cent01.ipv6lab.tw. 86400 IN      NS      ns1.cent01.ipv6lab.tw.
;; Received 101 bytes from 2001:c50:ffff:1::14#53(ns1.ipv6day.tw) in 2 ms

www.cent01.ipv6lab.tw. 86400 IN      AAAA    2404:0:40a1:0:215:5dff:fe50:f37b
cent01.ipv6lab.tw. 86400 IN      NS      ns1.cent01.ipv6lab.tw.
;; Received 129 bytes from 2404:0:40a1:0:215:5dff:fe50:f37b#53(ns1.cent01.ipv6lab.tw) in 0 ms
```

檢測IPv6反解

- 使用dig只透過IPv6檢查IPv6 AAAA反解
- **dig -x 2404:0:40a1:0:215:5dff:fe50:f37b -6 @2404:0:40a1:0:215:5dff:fe50:f37b**

```
[root@localhost ~]# dig -x 2404:0:40a1:0:215:5dff:fe50:f37b -6 @2404:0:40a1:0:215:5dff:fe50:f37b

;<<<> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6 <<<> -x 2404:0:40a1:0:215:5dff:fe50:f37b -6 @2404:0:40a1:0:215:5dff:fe50:f37b
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18669
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa. 86400 IN PTR www.cent01.ipv6lab.tw.
b.7.3.f.0.5.e.f.f.f.d.5.5.1.2.0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa. 86400 IN PTR ns1.cent01.ipv6lab.tw.

;; AUTHORITY SECTION:
0.0.0.0.1.a.0.4.0.0.0.4.0.4.2.ip6.arpa. 86400 IN NS ns1.cent01.ipv6lab.tw.

;; ADDITIONAL SECTION:
ns1.cent01.ipv6lab.tw. 86400 IN A 210.201.80.1
ns1.cent01.ipv6lab.tw. 86400 IN AAAA 2404:0:40a1:0:215:5dff:fe50:f37b

;; Query time: 1 msec
;; SERVER: 2404:0:40a1:0:215:5dff:fe50:f37b#53(2404:0:40a1:0:215:5dff:fe50:f37b)
;; WHEN: Wed Nov 13 14:41:53 2013
;; MSG SIZE rcvd: 201
```

上層ipv6lab.tw.正解授權設定

\$TTL 86400

\$ORIGIN ipv6lab.tw.

ipv6lab.tw. IN SOA ipv6lab.tw. root.localhost. (

2011030804 ; Serial

28800 ; Refresh

14400 ; Retry

720000 ; Expire

86400) ; Minimum

cent01 IN NS ns1.cent01.ipv6lab.tw.

ns1.cent01 IN A 210.201.80.1

ns1.cent01 IN AAAA 2404:0:40a1:0:215:5dff:fe50:f37b

mis.ipv6lab.tw.正解授權設定(cent01.ipv6lab.tw.zone)

\$TTL 86400

\$ORIGIN cent01.ipv6lab.tw.

cent01.ipv6lab.tw. IN SOA cent01.ipv6lab.tw. root.localhost. (

2013030402 ; Serial

28800 ; Refresh

14400 ; Retry

720000 ; Expire

86400) ; Minimum

mis IN NS ns1.mis.cent01.ipv6lab.tw.

ns1.mis IN A 210.201.80.41

ns1.mis IN AAAA 2404:0:40a1:0:c881:5840:7150:4cbe

48

Linux DNS BIND Named 啟動/停止/除錯

- 如何確定 DNS 是否運行呢？
 - ❑ 確認/var/log/messages是否出現異常訊息
 - ❑ 擷取host與server交換封包，確認封包交換是否成功
 - ❑ 檢視server回應訊息，確認封包之Rcode欄位之內容
 - ❑ Port Scan 目標 53/UDP
 - ❑ 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
 - ❑ 網路是否正常 (流量，斷線...)
 - ❑ 是否被 Router/Firewall 等擋掉了 port 53
 - ❑ 被入侵或欺騙
 - ❑ DNS 的指向錯誤(forward)

49

Named 啟動/停止/除錯

- 基本上只要執行named即可啟動DNS
 - ❑ # named 或
 - ❑ # /etc/rc.d/init.d/named start
 - ❑ named 啟動狀況會寫到 /var/log/messages中，只要查看這個檔案即可知道有無錯誤
- 要停止named，可直接kill掉其行程即可
 - ❑ # killall -9 named 或
 - ❑ # kill -9 pid-file 或
 - ❑ # /etc/rc.d/init.d/named stop
- 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)

50

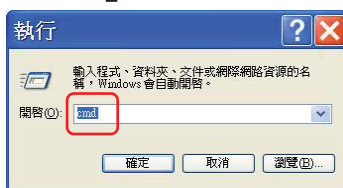
測試DNS 伺服器成功啟動IPv6與否

- 範例環境
 - ❑ 使用者端：
 - 使用啟動IPv6之桌上型電腦/筆記型電腦,例如Windows XP
 - ❑ DNS 伺服器
 - 假設其IPv4位址為1.2.3.4
 - 在正解檔資源記錄加入ns這台機器的A record與AAAA record

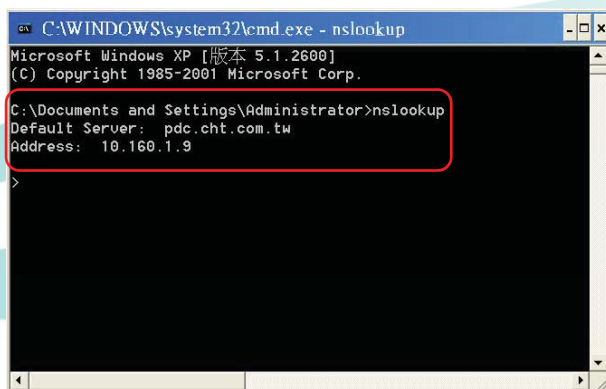
51

測試DNS伺服器-用戶端指令(1/3)

- Step1:[開始]->[執行]->輸入cmd於對話框中



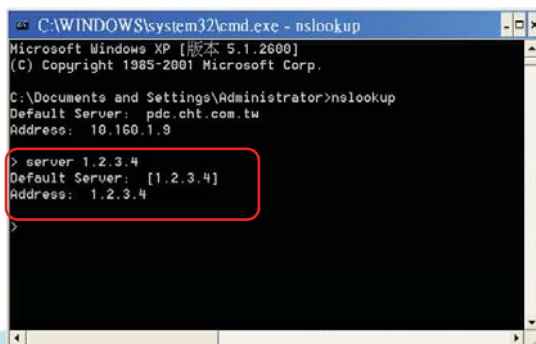
- Step2:於命令提示字元中輸入nslookup



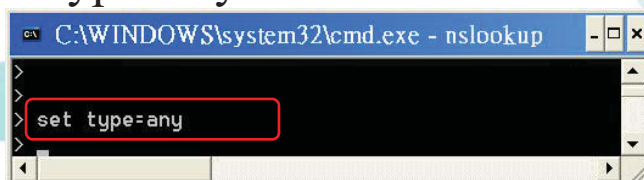
52

測試DNS伺服器-用戶端指令(2/3)

- Step3: 確定Default Server是啟動IPv6的那台DNS伺服器位址，可用"server 1.2.3.4"來修改Default Server



- Step4: 輸入"set type=any"設定要詢問所有種類的位址



53

測試DNS伺服器-用戶端指令(3/3)

nslookup

> set type=any

> www.cent01.ipv6lab.tw

Server: UnKnown

Address: 192.168.100.1

Non-authoritative answer:

www.cent01.ipv6lab.tw internet address = 210.201.80.1

www.cent01.ipv6lab.tw AAAA IPv6 address =
2404:0:40a1:0:215:5dff:fe50:f37b

54

WEB SERVER (APACHE)

55

Apache Server 安裝

- 在命令列使用yum安裝Apache

- #yum -y install httpd

```
[root@localhost ~]# yum -y install httpd
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
* base: ftp.twaren.net
* extras: ftp.twaren.net
* updates: ftp.twaren.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package httpd.i386 0:2.2.3-83.el5.centos set to be updated
-----<省略>-----
Installed:
  httpd.i386 0:2.2.3-83.el5.centos

Complete!
[root@localhost ~]#
```

Apache Server 設定及啟動

- 啟動Apache

- # /etc/init.d/httpd start

- 設定IPv6位址TCP 80 port

- 細部設定可編輯/etc/httpd/conf/httpd.conf

IPv6 防火牆-ip6tables

- 進行IPv6防火牆設定
 - 編輯ip6tables檔案，加入以下1行
 - # **vim /etc/sysconfig/ip6tables**
 - 編輯完成後，重新啟動IPv6防火牆
 - # **/etc/init.d/ip6tables restart**

```
[root@localhost ~]# vim /etc/sysconfig/ip6tables
-----<以上省略>-----
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
-----<以下省略>-----
[root@localhost ~]# /etc/init.d/ip6tables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading ip6tables modules: [ OK ]
Applying ip6tables firewall rules: [ OK ]
[root@localhost named]#
```

IPv4 防火牆-iptables

- 進行IPv4防火牆設定
 - 編輯iptables檔案，加入以下1行
 - # **vim /etc/sysconfig/iptables**
 - 編輯完成後，重新啟動IPv4防火牆
 - # **/etc/init.d/iptables restart**

```
[root@localhost ~]# vim /etc/sysconfig/iptables
-----<以上省略>-----
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
-----<以下省略>-----
[root@localhost ~]# /etc/init.d/iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]
[root@localhost named]#
```

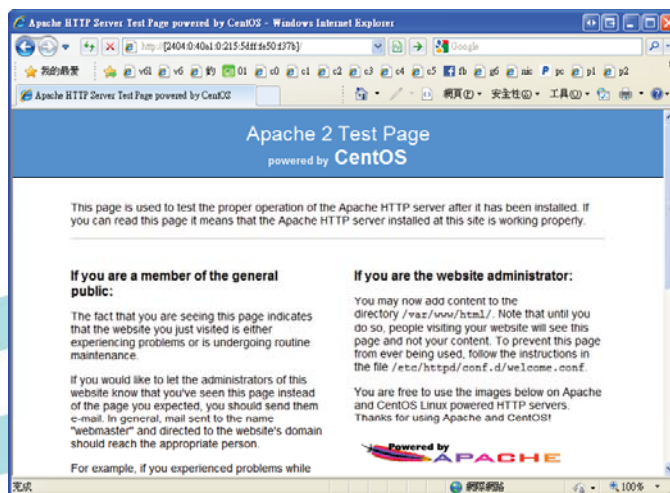
IPv6 Web Server 測試

- 驗證網站伺服器已開啟IPv6服務

□ # **netstat -an | grep :80 | grep LISTEN**

```
tcp        0      0 :::80               :::*                  LISTEN
```

- 連線開啟IPv6測試網站



Thank You