臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告
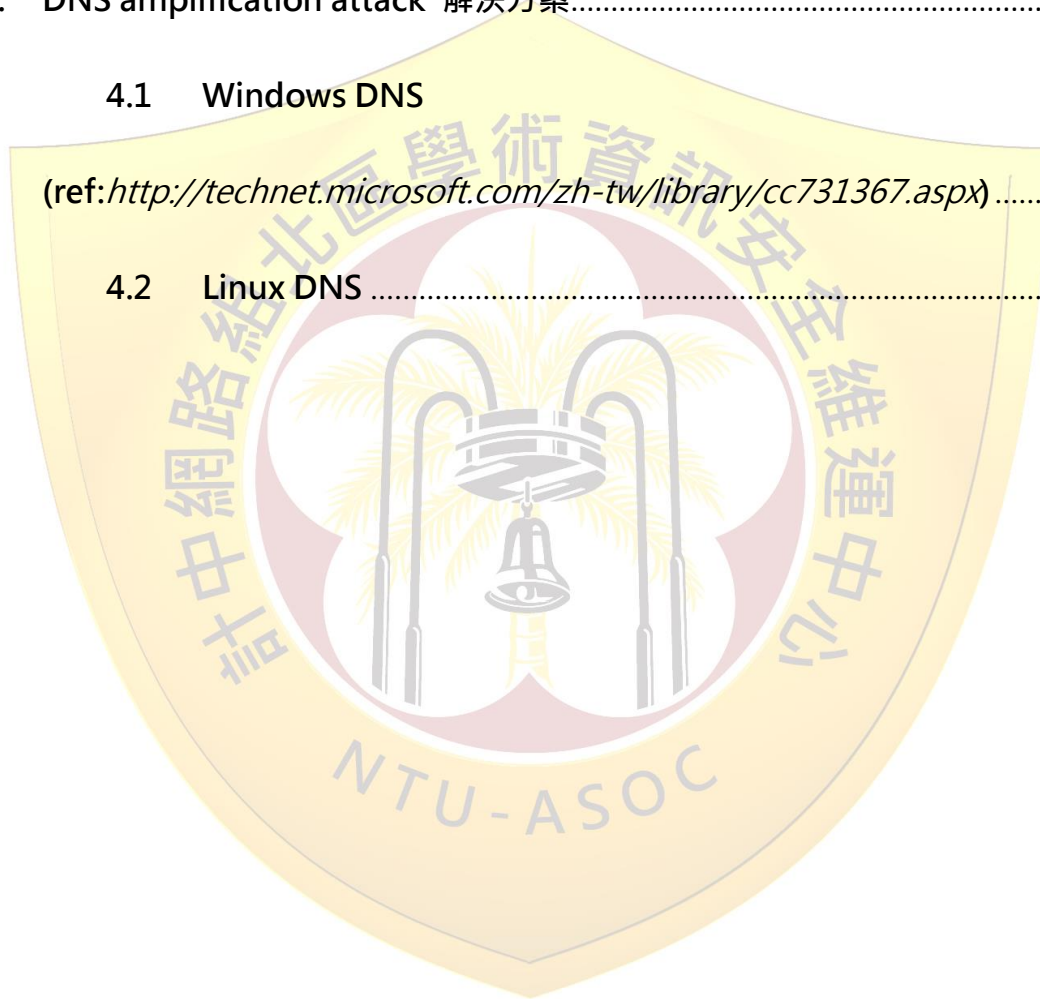
DNS amplification attack

分析報告

北區 ASOC 團隊製

2013/11

1. DNS 簡介

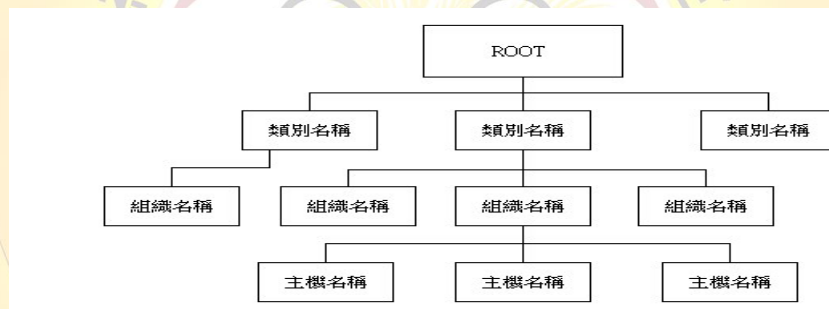在早期 TCP/IP 協定的網路環境中，兩台主機間若要進行通訊，則必須

先知道對方的 IP 位址，才能開始網路通訊，而人們對於純數字的 IP 格

式資料的記憶並不在行，DNS 服務就是為了解決這問題而生，DNS 全名為

Domain Name Service，主要的用途在於將一般人易於記憶的網址轉換成

電腦所使用的 IP 格式，而 DNS 其實沒有想像中的遙遠，當打開瀏覽器鍵入

網址連上網時，其實已經在使用 DNS 的服務了。

DNS 系統基本是採樹狀階層式(hierarchy)，類似 Windows 中的

目錄樹結構，最頂層的有數十個 root DNS servers，記錄著所有最頂層 DNS

server 資料，稱為" root" 或根目錄，接著下分為幾個基本的類別，如:com、

org、edu。因網際網路的蓬勃發展，在此層級，也加入國別代號，如 tw(台
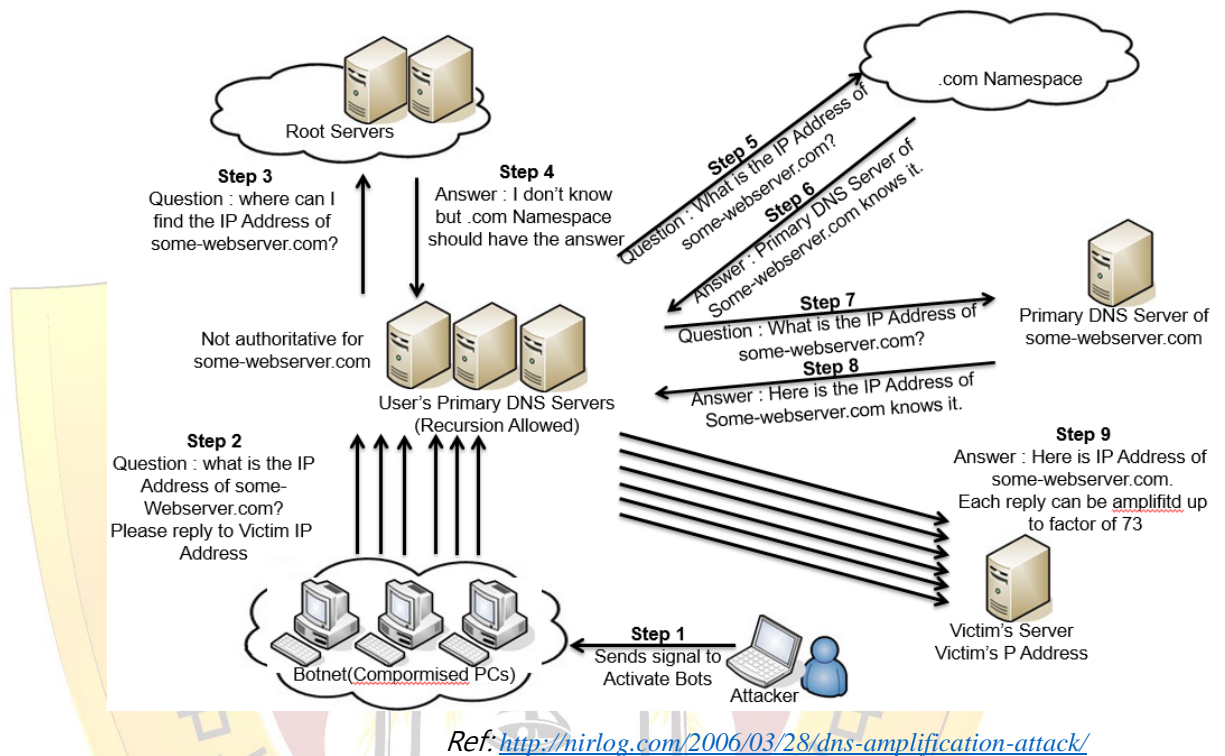
灣)、hk(香港)、jp(日本)，而美國則是因為當初發展制定 Internet 規範，則

沒有國域名稱，再往下便是組織名稱，如 google、facebook、yahoo...等

等，繼組織名稱後，便是主機名稱，如 www、mail、ftp...等等，所以一個

完整的 dns 名稱就會像是:

www(*主機名稱*).google(*組織名稱*).com(*國別代號因美國而省略*)。

2. DNS amplification attack(放大攻擊)簡介

Ref: http://nirlog.com/2006/03/28/dns-amplification-attack/

DNS 放大攻擊可參考上圖來了解攻擊的流程與資料流的方向。

- Step 1：攻擊者向已受控制的殭屍電腦群下達開始攻擊指令。

- Step 2：遭感染的殭屍電腦群向未做好安全設定的 DNS server

  發出偽造的 DNS query 封包，偽造成受害者的 IP 位址為來源位址進行遞迴查詢(recursive query)。

● Step 3：受害的 DNS 主機向根目錄 Server 進行 domain 查

詢。

● Step 4：根目錄主機向受害 DNS 主機回傳查詢無此

domain 的

訊息，並回傳另一根伺服器可能有其 domain 資料。

● Step 5：受害 DNS 主機轉向另一根目錄 Server 進行

domain 查

詢。

● Step 6：外部根目錄 Server 回傳知道此 domain 資料的

DNS

server 位址。

● Step 7：受害 DNS 主機再度向此 DNS 發出查詢。

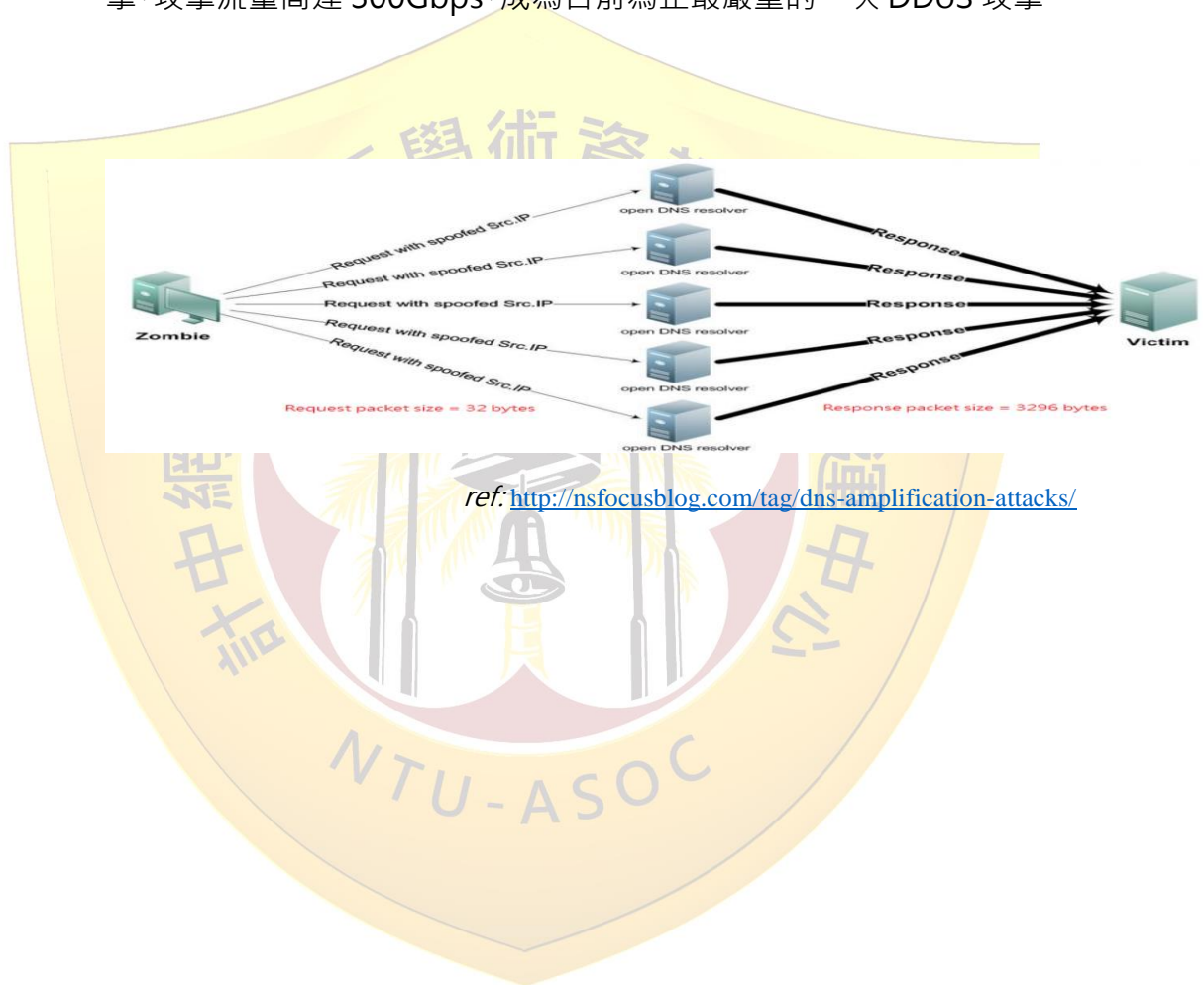● Step 8：外部 DNS 回傳受害 DNS 主機 domain 查詢資

料。

● Step 9：受害 DNS 主機向遭偽造來源的主機回傳

domain 查詢

資料。

攻擊者透過不斷重複上述步驟，向目標主機發送大量 UDP 封包，

藉此阻斷其正常服務，也由於受害 DNS 主機回傳到目標主機之封包大

小會大於殭屍電腦群所發送的封包大小，過程中流量具有放大的效果，

故稱其為 DNS 放大攻擊。

2013 年三月歐洲反垃圾郵件組織 Spamhaus 即是遭此 DDoS 攻

擊，攻擊流量高達 300Gbps，成為目前為止最嚴重的一次 DDoS 攻擊。

*ref:*http://nsfocusblog.com/tag/dns-amplification-attacks/

參考上圖可了解此種攻擊模式下的放大效果，約可從 32byte(*殭屍電腦群發出*)放大至 3296byte(*DNS 主機回傳給受害主機*)，攻擊頻寬約可被放大 100 倍左右，當殭屍電腦群發出大量的 DNS query 封包時，甚至會導致封包在 router 轉送時出現壅塞，進而產生更大規模的影響，所以 DNS 主機安全性設定，已成為不可忽視的重要課題之一。

3. DNS amplification attack 分析說明
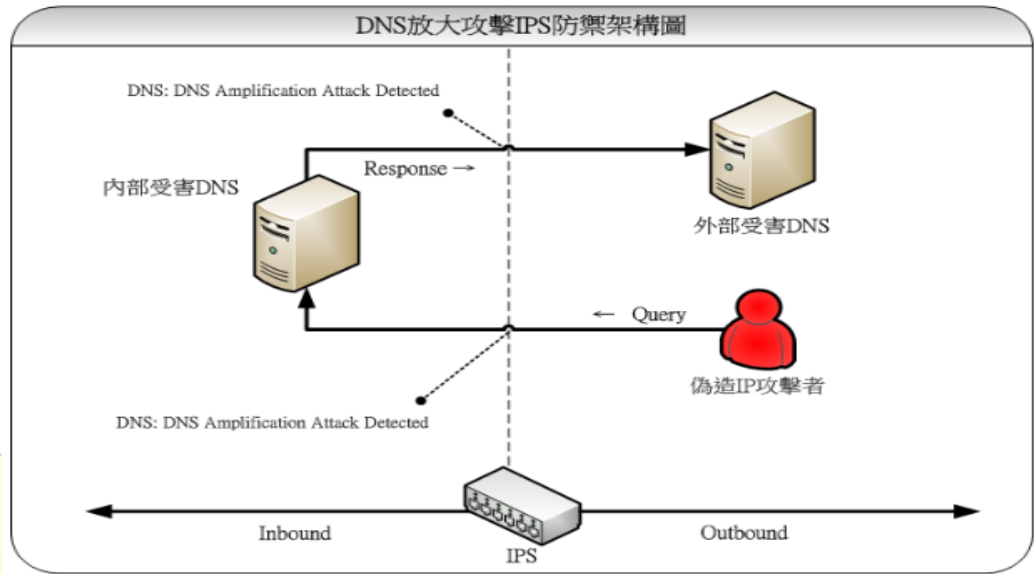
　　北區 ASOC 透過 IPS 即時監測各區網中心是否有 DNS 放大攻擊事件，偵測基本架構可參考上圖，透過於網路骨幹中的 IPS，同時檢測 Inbound 及 Outbound 的流量，一旦有外部攻擊者發出偽造來源的惡意 DNS 封包或內部 DNS 主機發出異常 query 封包時，皆可被 IPS 偵測到，避免 DDoS 攻擊之情事發生，在此種偵測模式下，我們可以確保轄下連線單位內的 DNS 不被外部惡意攻擊者所利用，同時，也能確保內部不受到此種攻擊模式危害，在大規模攻擊情事發生前，亦能提早發出告警，避免攻擊進一步擴大而影響整體網路環境。
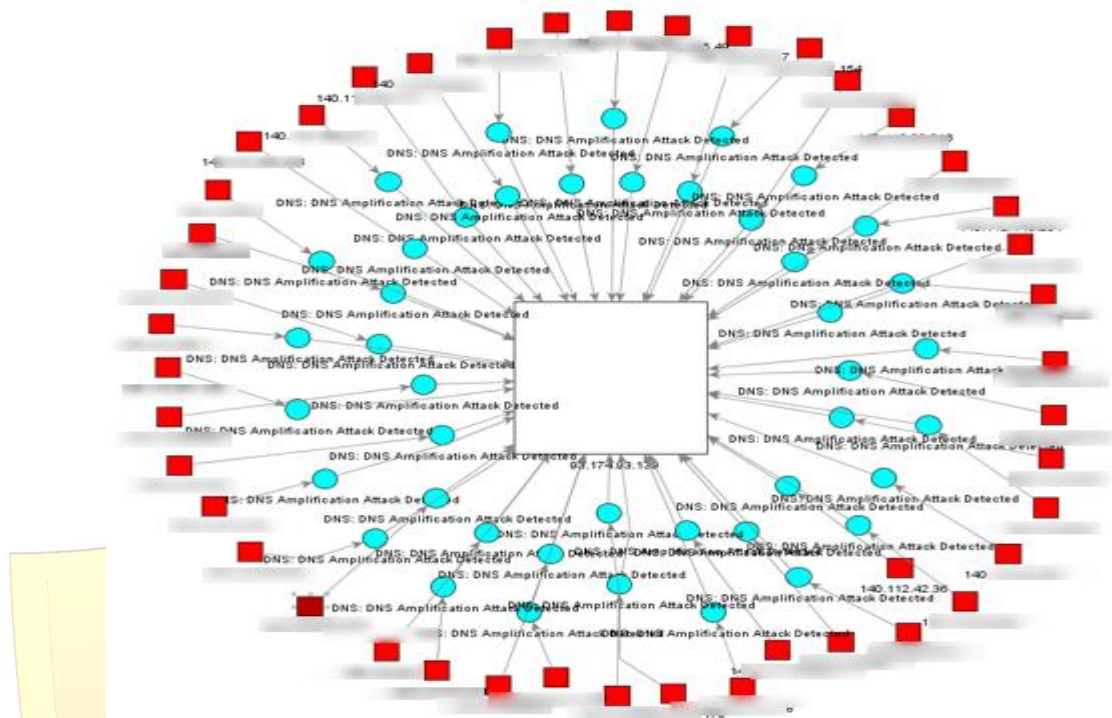
　　經過 Arcsight 收容前端 IPS 資料後，進行後續的關聯分析，產出如上攻擊拓撲圖，可了解此種攻擊行為的模式及其關連性。其中紅色方形代表攻擊發動者，藍色圓形表示攻擊事件類型，而白色方形代表攻擊目的端主機，圖形的大小代表攻擊量的多寡，綜合以上資訊，可以發現 DNS 放大攻擊模式具有多攻擊來源、單一目標、及龐大數量等特性。在此模式下，目標主機若沒有相關防護措施，網路環境很容易被攻擊造成網路癱瘓。

　　檢視 IPS 所偵測到的事件封包如上圖所示，可發現具有明確的

攻擊特徵，攻擊者偽造來源後，並針對特定 domain 發送大量 query 封包，

正常使用者不應發出如此頻繁的 DNS query，且查詢的 Domain name 皆

為"sandia.gov"，明顯為異常行為的 DNS 放大攻擊。

4. DNS amplification attack 解決方案

4.1 Windows DNS (ref:*http://technet.microsoft.com/zh-tw/library/cc731367.aspx*)

為避免 DNS 主機被利用為攻擊的跳板，建議 DNS 設定須符

合下列兩項安全性設定:

- *設定 ACL，僅允許符合 ACL 設定的網段進行 recursive query 或關閉 recursive query*

設定 ACL

1. 開啟 [DNS 管理員]。
2. 在主控台樹狀目錄中按一下適用的 DNS 伺服器。

位置

- *DNS/適用的 DNS 伺服器*

3. 在 [**執行**] 功能表，按一下 [**內容**]。
4. 在 [**介面**] 索引標籤上，按一下 [**只有下列 IP 位址**]。
5. 在 [**IP 位址**] 中，輸入為此 DNS 伺服器啟用的 IP 位址，然後按一下 [**新增**]。
6. 視需要重複上一個步驟，以指定為此 DNS 伺服器啟用的其他伺服器 IP 位址。

若要從清單移除 IP 位址，然後按一下 [**移除**]。

或使用命令列執行:

1. 開啟命令提示字元。
2. 輸入下列命令，再按 ENTER 鍵：

```
dnscmd <ServerName> /ResetListenAddresses
[<ListenAddress> ...]
```

關閉 recursive query

1. 開啟 [DNS 管理員]。

2. 在主控台樹狀目錄的適當 DNS 伺服器上按一下滑鼠右鍵，然後按一下 [內容]。

位置

DNS/*適用的 DNS 伺服器*

3. 按一下 [進階] 索引標籤。

4. 在 [伺服器選項]中，選取 [停用遞迴] 核取方塊，然後按一下 [確定]。
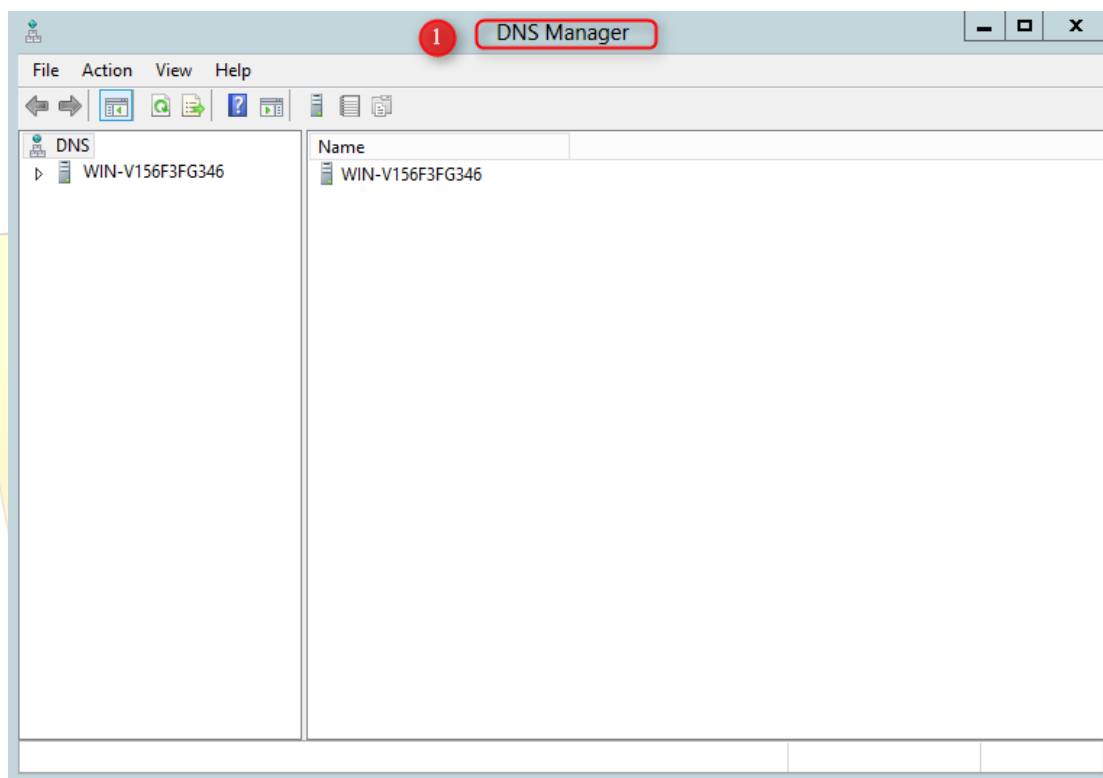
或使用命令列執行:

1. 開啟命令提示字元。

2. 輸入下列命令，再按 ENTER 鍵：

```
dnscmd <ServerName> /Config /NoRecursion {1|0}
```
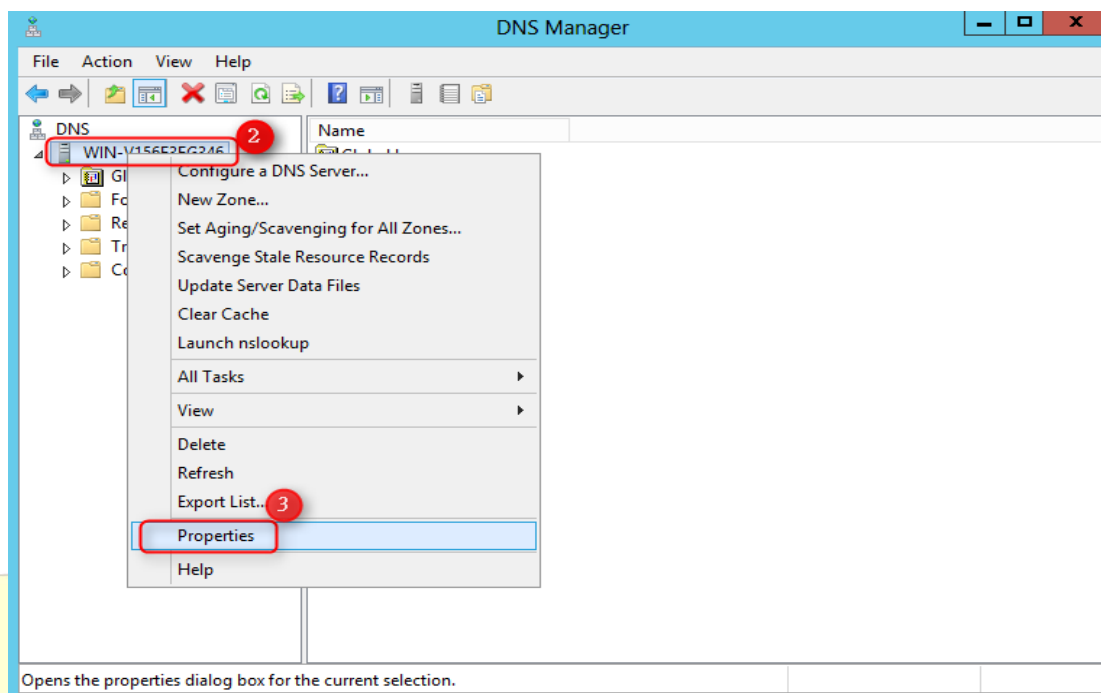
以各 Windows 版本作業系統實作為例:
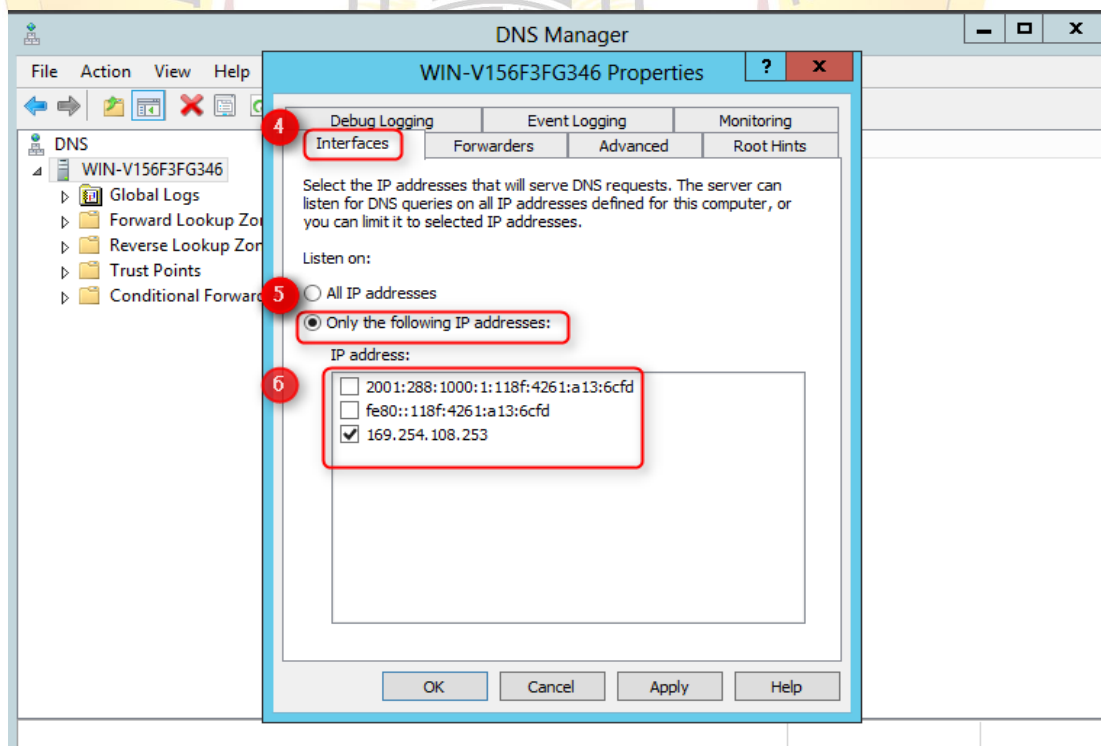
Windows 2012

1.開啟 DNS Manager

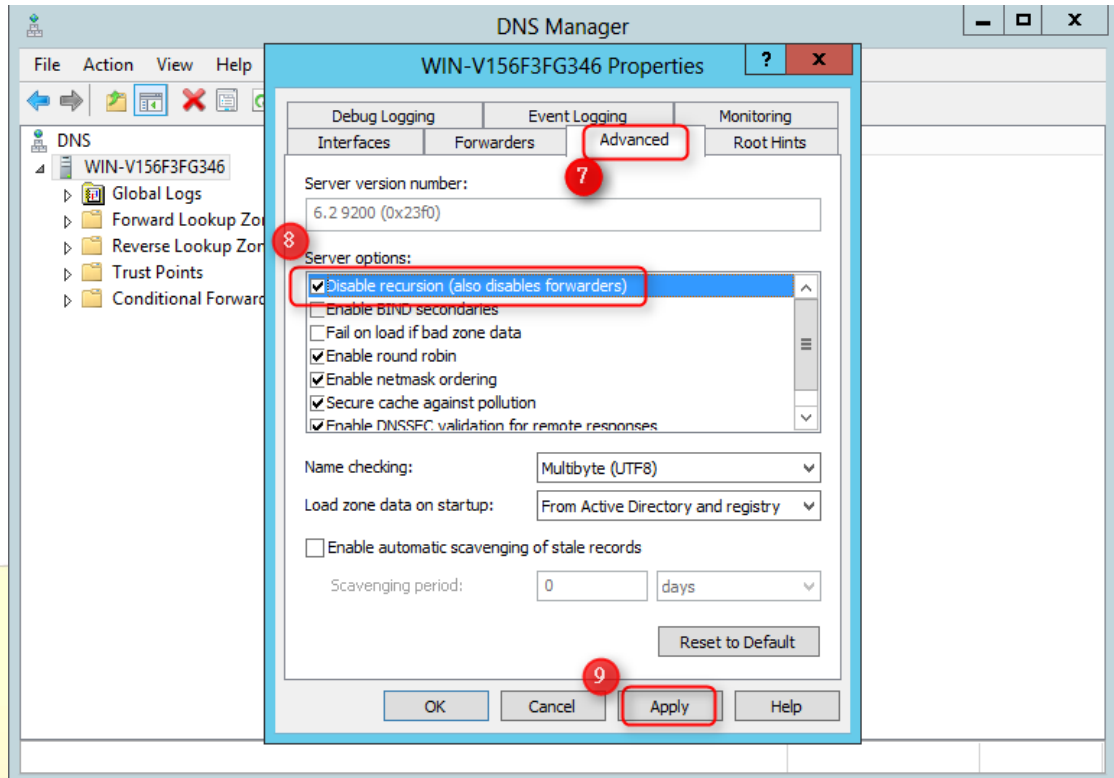*2.選擇 DNS 伺服器名稱右鍵>內容*

3.選擇屬性

4.選擇〞**介面**〞標籤頁

5.選擇僅有下列 *IP* 可以連線

6.勾選允許連線之介面

7.選擇〞**進階**〞標籤頁

8.勾選**停用遞迴**查詢選項

9.選取〞**套用**〞

CMD 操作模式如下:

1. 設定查詢 ACL
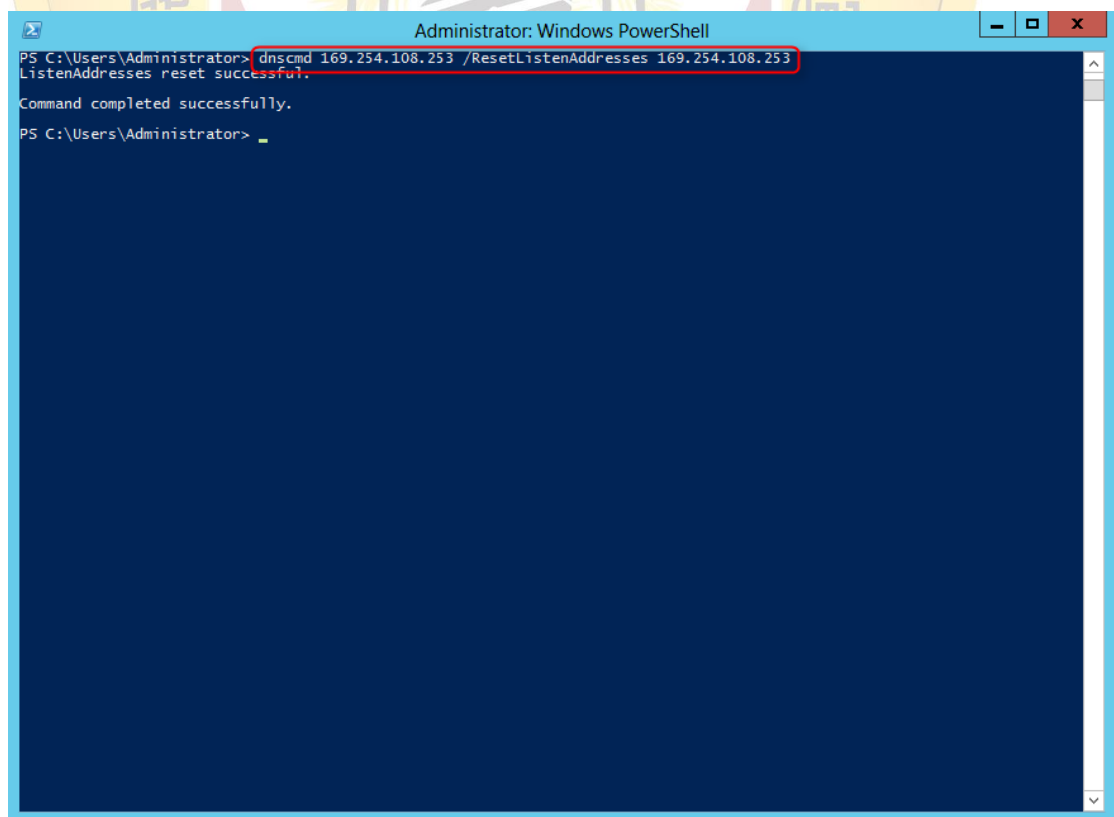
2. 關閉遞迴查詢

PS C:\Users\Administrator> dnscmd 169.254.108.253 /Config /NoRecursion {0}

Registry property NoRecursion successfully reset.
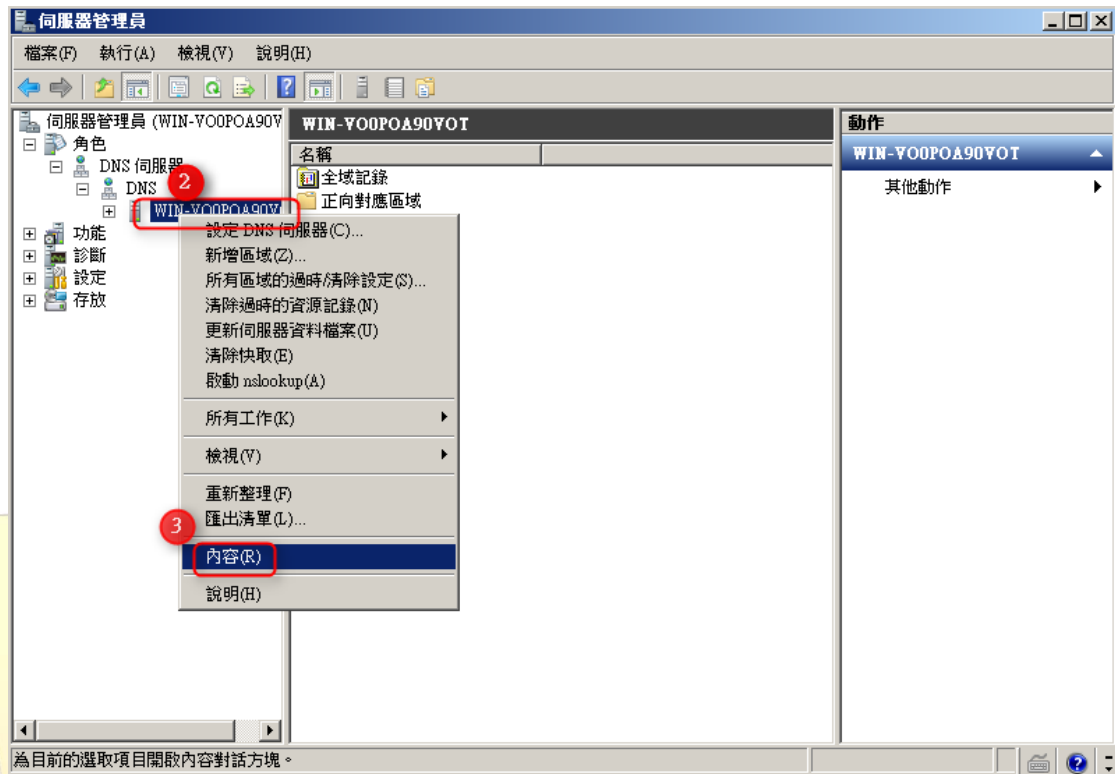Command completed successfully.
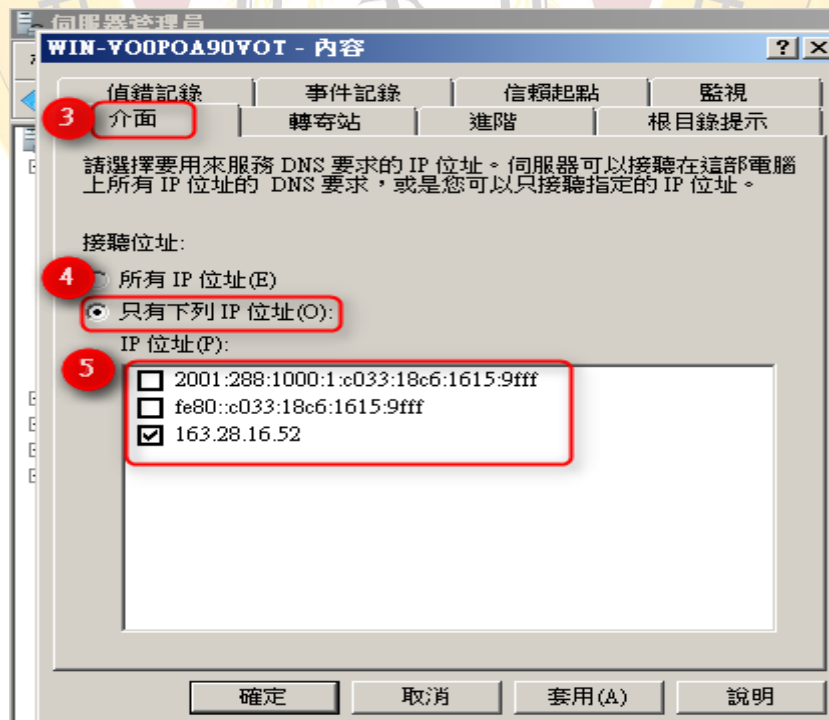
PS C:\Users\Administrator>

Windows 2008

1.執行伺服器管理員

伺服器管理員 **1**

檔案(F)　執行(A)　檢視(V)　說明(H)

伺服器管理員 (WIN-VO0POA90VOT)
角色
　DNS 伺服器
　　DNS
　　　WIN-VO0POA90VOT
功能
診斷
設定
存放

角色

檢視在此伺服器上安裝的角色健康情況並新增或移除角色和功能。

⌃ 角色摘要　　　　　　　　　　　? 角色摘要說明

⌃ 角色: 已安裝 17 之 1　　　　　　新增角色
　　　　　　　　　　　　　　　　移除角色
　❌ DNS 伺服器

⌃ DNS 伺服器　　　　　　　　　? DNS 伺服器 說明

提供 TCP/IP 網路的名稱解析。

⌃ 角色狀態　　　　　　　　　　移至 DNS 伺服器

　　訊息: 無
　　系統服務: 全部執行中
　❌ 事件: 在過去 24 小時 內: 48 個錯誤, 2
　　個警告, 17 個資訊
　　Best Practices Analyzer: 若要啟動 Best
　　Practices Analyzer 掃描，請移至這個角
　　色首頁上的 Best Practices Analyzer 方
　　塊，然後按一下 [掃描這個角色]。

上次重新整理時間: 今天 下午 03:07　設定重新整理

16

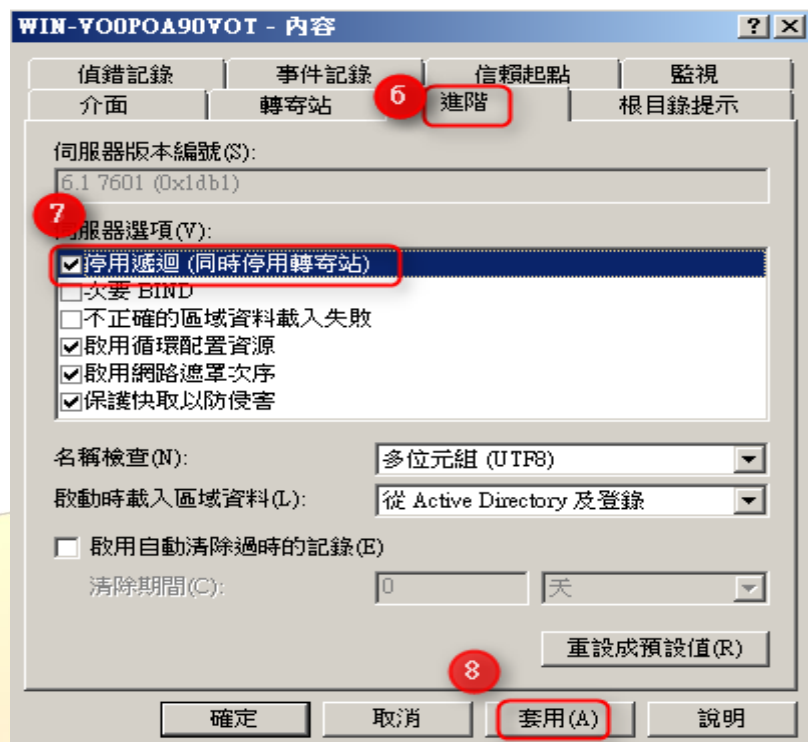*2.選取 DNS 伺服器後，點選右鍵>內容*

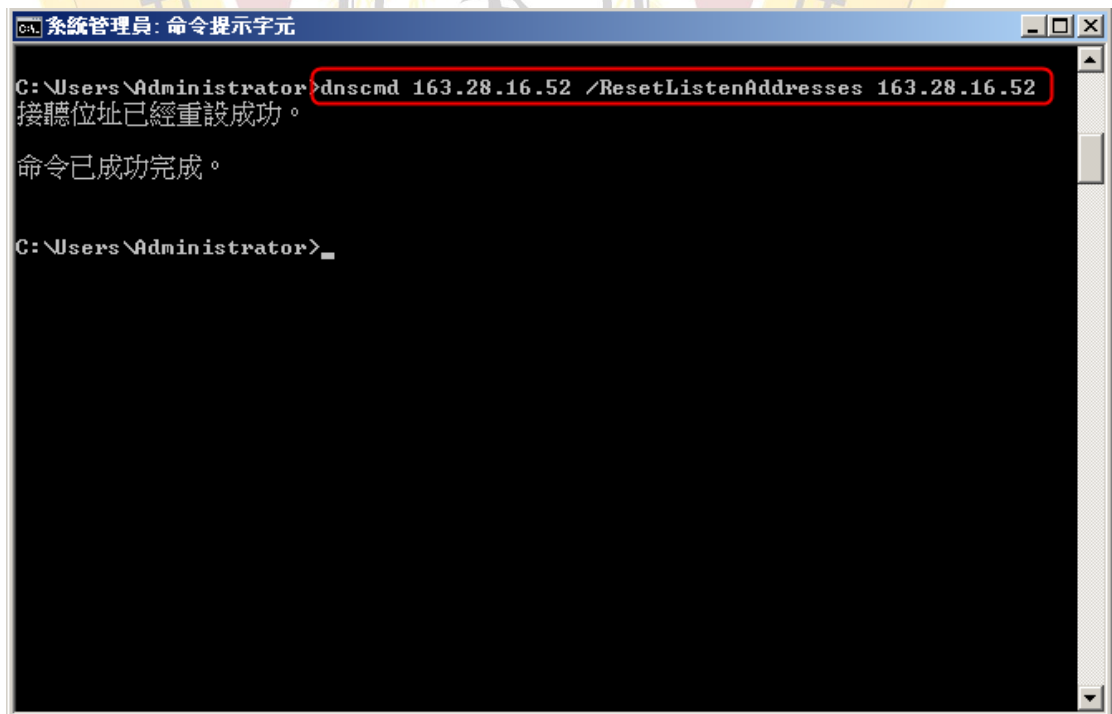*3.選取"介面"標籤頁*

4.選擇只有下列 IP 位址

5.勾選允許連線之介面

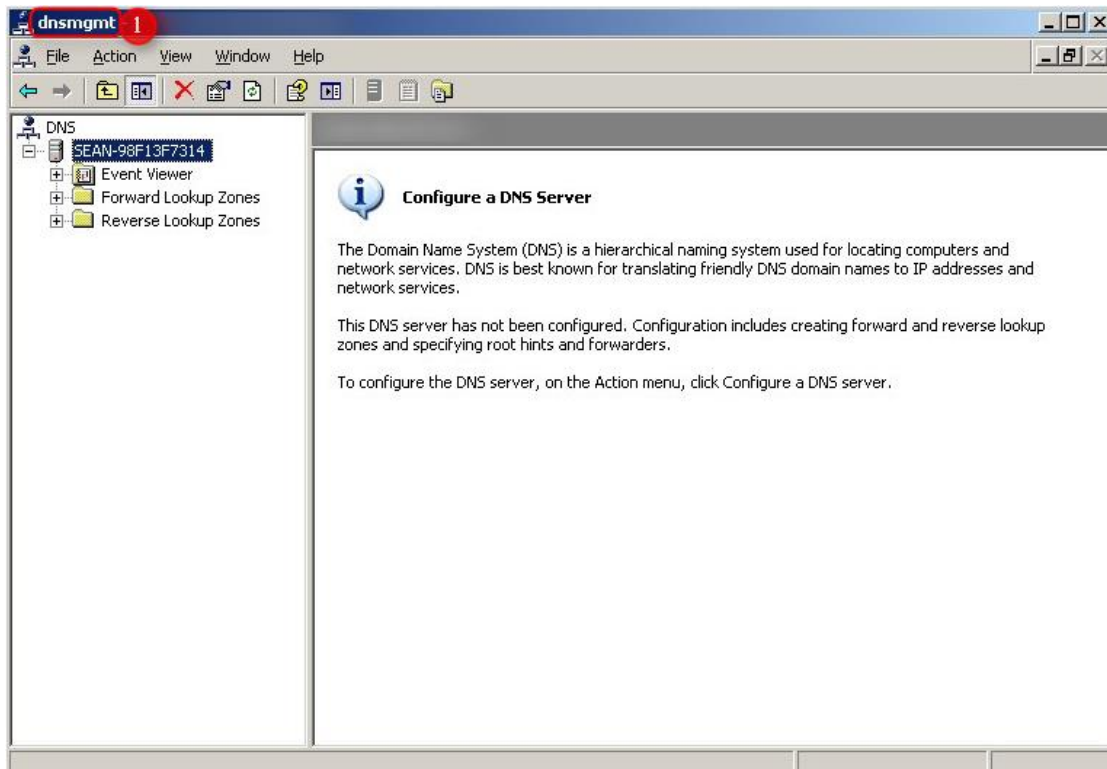*6.選擇"進階"頁面*

7.勾選"停用遞迴"

CMD 操作模式如下:

1. 設定查詢 ACL

2. 關閉遞迴查詢

系統管理員: 命令提示字元

```
C:\Users\Administrator>dnscmd 163.28.16.52 /Config /NoRecursion 0

登錄內容 NoRecursion 已經重設成功。
命令已成功完成。


C:\Users\Administrator>
```
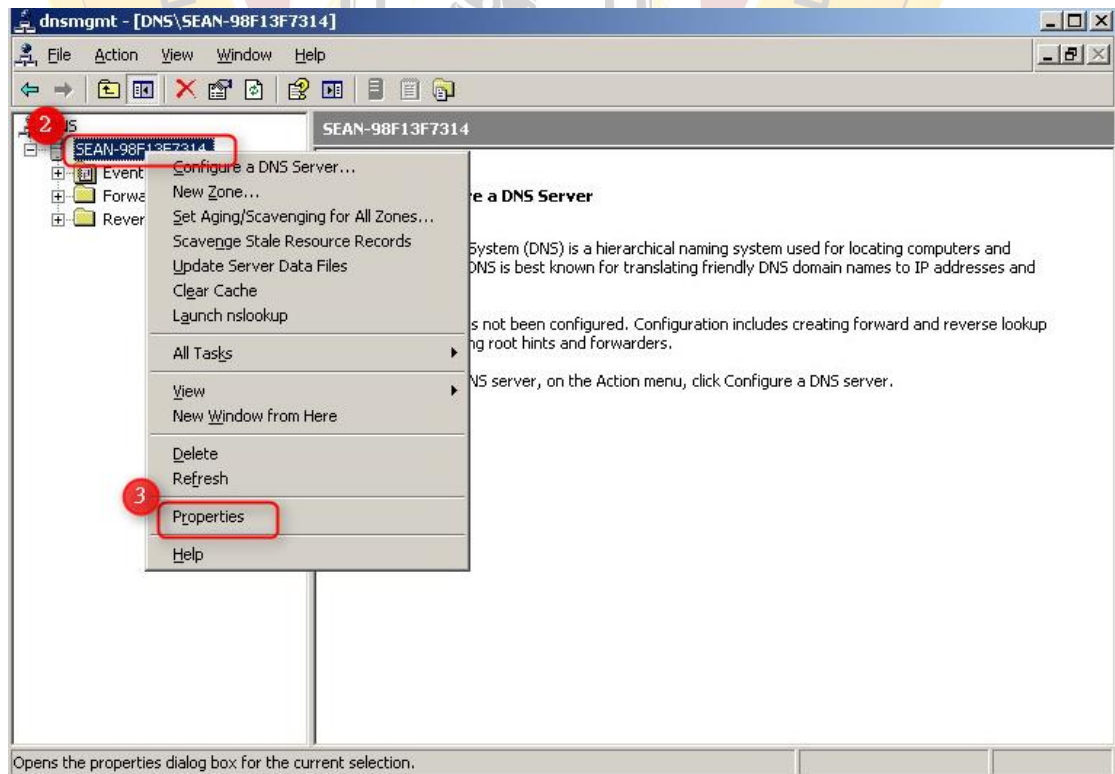
Windows 2003

1.執行 DNS 管理員
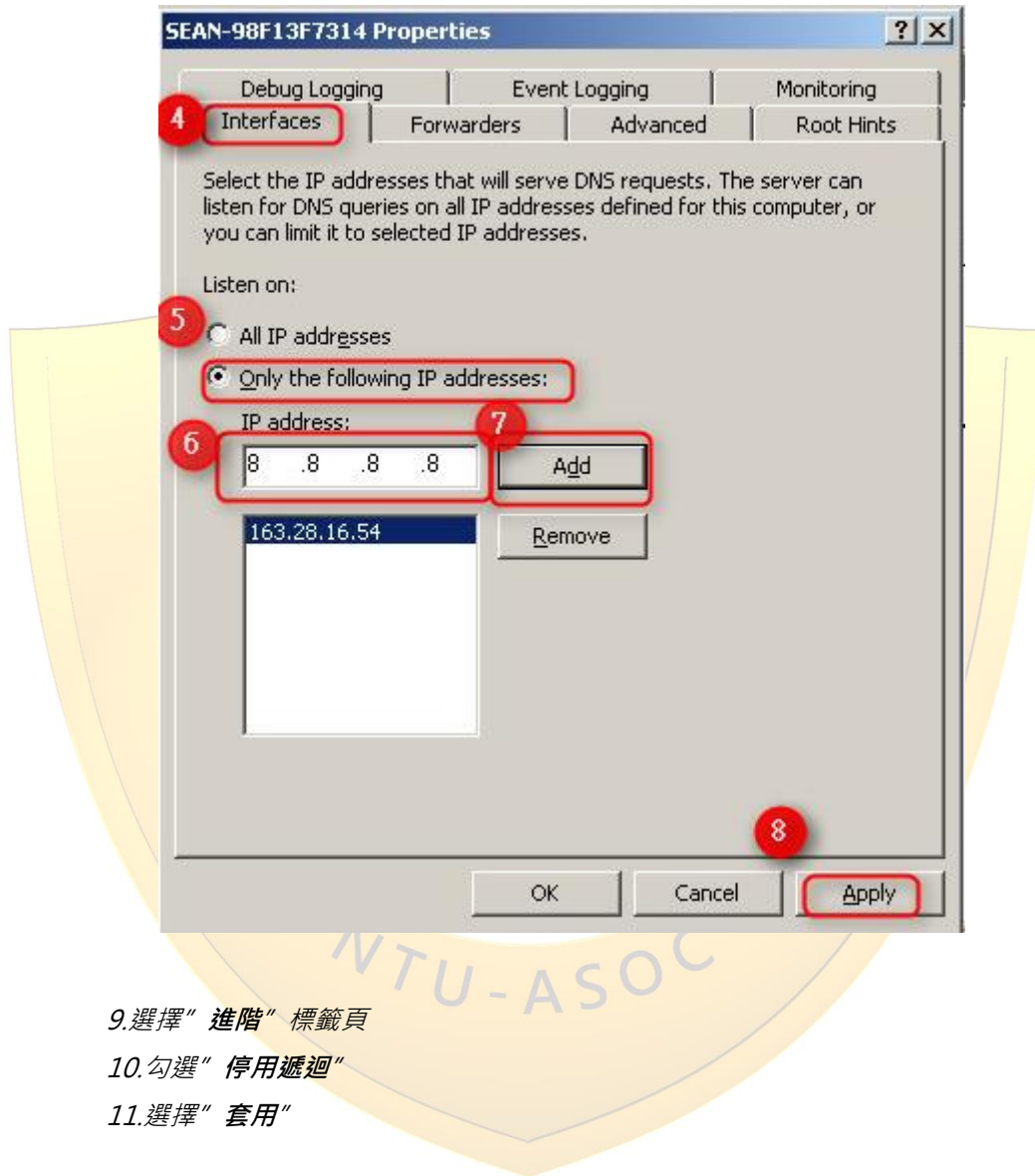

2.選擇 DNS 伺服器，右鍵>內容

3.選擇" 內容"

4.選擇"介面"標籤頁
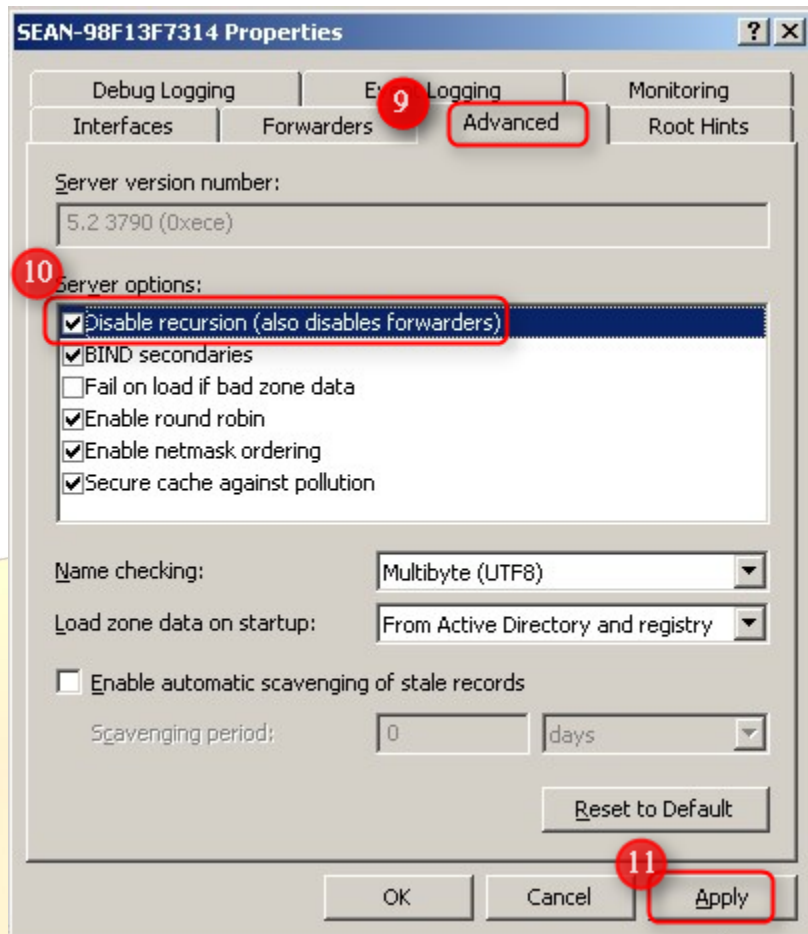
5.選擇只有下列 IP 位址

6.輸入允許連線之 IP 位址

*7.點擊"**新增**"*

*8.選擇"**套用**"*

*9.選擇"**進階**"標籤頁*

*10.勾選"**停用遞迴**"*

*11.選擇"**套用**"*

4.2 Linux DNS

為避免 DNS 主機被利用為攻擊的跳板，建議 DNS 設定須符

合下列兩項安全性設定:

- *在 BIND 版本 9.5 之前，recursion 的功能是預設開啟的，故管理者必須自行關閉此功能或設定適當的存取權限。*
- *以下為 BIND 的組態設定檔 Name.conf 的建議設定*

/*定義一個 ACL，設定能存取 DNS 服務的 IP 範圍，此例 192.168.0.0/16，可自行調整為貴單位的網段*/

Acl "allowed-IP"{

* 192.168.0.0/16;*

};

/*僅允許符合 ACL 設定的網段進行 recursive query*/

Options {

……

Allow-recursion { allowed-IP; };

……

};

/*提供貴單位管轄下的網域給其它 DNS 查詢*/

zone "XXX.edu.tw" in {

*   ……*

allow-query { any; };

……

};

而更多詳細的設定步驟可參考:

https://kb.isc.org/category/116/0/10/Software-Products/BIND9/Documentation/